May 2020

Localizing Spoofing Attacks on Vehicular GPS Using Vehicle-to-Vehicle Communications

Christian Titus Sanders
Clemson University, ctsande@g.clemson.edu

Localizing Spoofing Attacks on Vehicular GPS Using Vehicle-to-Vehicle Communications

---

A Dissertation
Presented to
the Graduate School of
Clemson University

In Partial Fulfillment
of the Requirements for the Degree
Master of Science
Electrical Engineering

---

by
Christian Sanders
May 2020

Accepted by:
Dr. Yongqiang Wang, Committee Chair
Dr. Harlan Russell
Dr. Kuangching Wang

Abstract

GPS spoofing is a problem that is receiving increasing scrutiny due to an increasing number of reported attacks. Plenty of results have been reported on detecting the presence of GPS spoofing attacks. However, very few results currently exist for the localization of spoofing attackers, which is crucial to counteract GPS attacks. In this paper we propose leveraging vehicle-to-vehicle communications to detect and localize spoofing attacks on vehicular navigation GPS. The key idea is to correlate Doppler shift measurements which are reported by most commercial GPS receivers. The approach does not need additional dedicated devices and is easily deployable on modern vehicles equipped with vehicle-to-vehicle communication devices. It is capable of localizing both stationary spoofers and mobile spoofers which could be mounted on a vehicle. Both numerical simulations and experimental tests are conducted to confirm the effectiveness of the proposed approach.

Acknowledgments

First and foremost, I would like to thank my committee chair, Dr. Yonqiang Wang, for his continual guidance and mentorship throughout this entire process. I would also like to thank David Lynge, who's assistance early in the experiments proved invaluable. Finally, I am grateful to both Dr. Harlan Russell and Dr. Kuangching Wang for agreeing to be a part of my committee.

Table of Contents

Title Page . . . . . **i**

Abstract . . . . . **ii**

Acknowledgments . . . . . **iii**

List of Tables . . . . . **v**

List of Figures . . . . . **vi**

1 Introduction **1**
1.1 Overview of the Problem 1
1.2 GPS background 1
1.3 GPS Attacks 4
1.4 Literature Review on Detection of GPS Spoofing 5

2 Models and Approach **7**
2.1 Attacker Model 7
2.2 Victim Model 8
2.3 Approach 8

3 Evaluation Based on Numerical Simulations **17**
3.1 Simulation Setup 17
3.2 Influence of Number of Samples 19
3.3 Influence of Parallel Distance, h 22
3.4 Influence of Perpendicular Distance, A 23
3.5 Influence of the Relative Vehicle Distance, D 24

4 Evaluation Based on Experiments **31**
4.1 Experimental Setup 31
4.2 Experimental Results: Stationary Spoofer 32
4.3 Experimental Results : Mobile Spoofer 38

5 Conclusions **42**
5.1 Evaluation of Results 42
5.2 Future Work 43
5.3 Conclusions 44

Bibliography **45**

List of Tables

1.1 Commercial GPS receivers reporting Doppler shift 5

List of Figures

1.1 A diagram describing the basic process for use of multilateration to determine receiver position from [40]. 2

2.1 A diagram of the receivers and the attacker. There are two receivers, 1 and 2, each of which takes measurements at m different instances of measuring time. Each receiver has knowledge of the speed it is moving at each time as well as the distance it has traveled since the first measurement. 9

3.1 A diagram of the spoofer setup used in numerical simulations. 17
3.2 Typical simulation results for the stationary spoofer case. 19
3.3 Typical simulation results for the moving spoofer case. 20
3.4 The influence of the number of samples (m) on localization performance in the static spoofer case. 21
3.5 A diagram of the formation examined where the attacker moves at a 45 degree angle with the receivers. Only two receivers are shown here due to space constraints. . . . 22
3.6 A diagram of the formation of the receivers moving in the opposite direction of the attacker on the same road. 22
3.7 The influence of the number of samples (m) on localization performance in the moving spoofer case illustrated in figure 3.5. 23
3.8 The influence of the number of samples (m) on localization performance in the moving spoofer case illustrated in figure 3.6. 24
3.9 The influence of the distance h on the localization performance for the static spoofer case. 25
3.10 The influence of the distance h on the localization performance for the moving spoofer case illustrated in figure 3.5. 26
3.11 The influence of the attacker distance, A, on the localization performance in the static spoofer case. 27
3.12 The influence of the attacker distance, A, on the localization performance for the moving spoofer case illustrated in figure 3.5. 28
3.13 The influence of the relative receiver distance, D, on localization performance for the static spoofer case. 29
3.14 The influence of the relative receiver distance, D, on localization performance for the moving spoofer case. 30

4.1 A diagram of the basic experimental setup. The USRP B210 simultaneously transmits signals over two channels to two separate GPS receivers. These would be shielded in aluminum to prevent signal leakage. 32
4.2 The average calculation error at different distances from the attacker and different relative vehicle distances. 33
4.3 The average calculation error at additional distances from the attacker and different relative vehicle distances. 34

4.4 The ratio of the average calculation error to the distance from the attacker to the receivers. 35
4.5 The average calculation error at different perpendicular distances from the attacker and different relative vehicle distances. 36
4.6 The average calculation error at additional perpendicular distances from the attacker and different relative vehicle distances. 37
4.7 The ratio of the average calculation error to the distance from the attacker to the receivers at different relative receiver distances. 38
4.8 The average error calculated for each position based on experiments for the moving spoofer on the same road in the opposite direction of the victims. 39
4.9 The average error calculated for each position based on experiments for the moving spoofer moving at a 45 degree angle relative to the victims. 40

Chapter 1

Introduction

1.1 Overview of the Problem

The global positioning system (GPS) has become a crucial navigation system for all kind of transportation systems, ranging from planes to ships to cars or even on phones for pedestrians. Furthermore, GPS can also be used for accurate time acquisition, which is crucial for the operation of power systems, banking systems, and stock exchange. Unfortunately, despite being ubiquitous and vital in modern society, GPS is also vulnerable to attacks for a couple of reasons. First, commercial GPS receivers are unable to use encrypted signals from GPS satellites and have to rely on unencrypted messages, which are easy to replicate for an attacker. Also, due to the long distance from GPS satellites to ground GPS receivers, the signals reaching the receivers are extremely weak. In fact, the power of GPS signals received on the Earth is as low as 10^{-16} Watts [24]. Thus, an attacker can easily transmit a stronger signal and drown out the authentic signal.

1.2 GPS background

GPS functions by having a constellation of satellites of known position circling the Earth. Each satellite transmits a unique signal down towards GPS receivers located on the Earth. When the receivers process the signals they can determine the time from when the satellite transmitted the signal to when the signal reached the receiver. By multiplying this time by the speed of light,

as seen in equation 1.1, the distance from the satellite can be calculated.

$$r_i = c(t_u - t_{si}) \tag{1.1}$$

In this equation, r_i represents the distance from the receiver to satellite i, c represents the speed of light, t_u is the time the signal reaches the receiver, and t_{si} is the time that receiver i transmits the signal. If three satellites are visible to the receiver simultaneously, the receiver could determine the distance to each satellite and then use the process of multilateration to determine its own position. A diagram of this can be seen in figure 1.1.

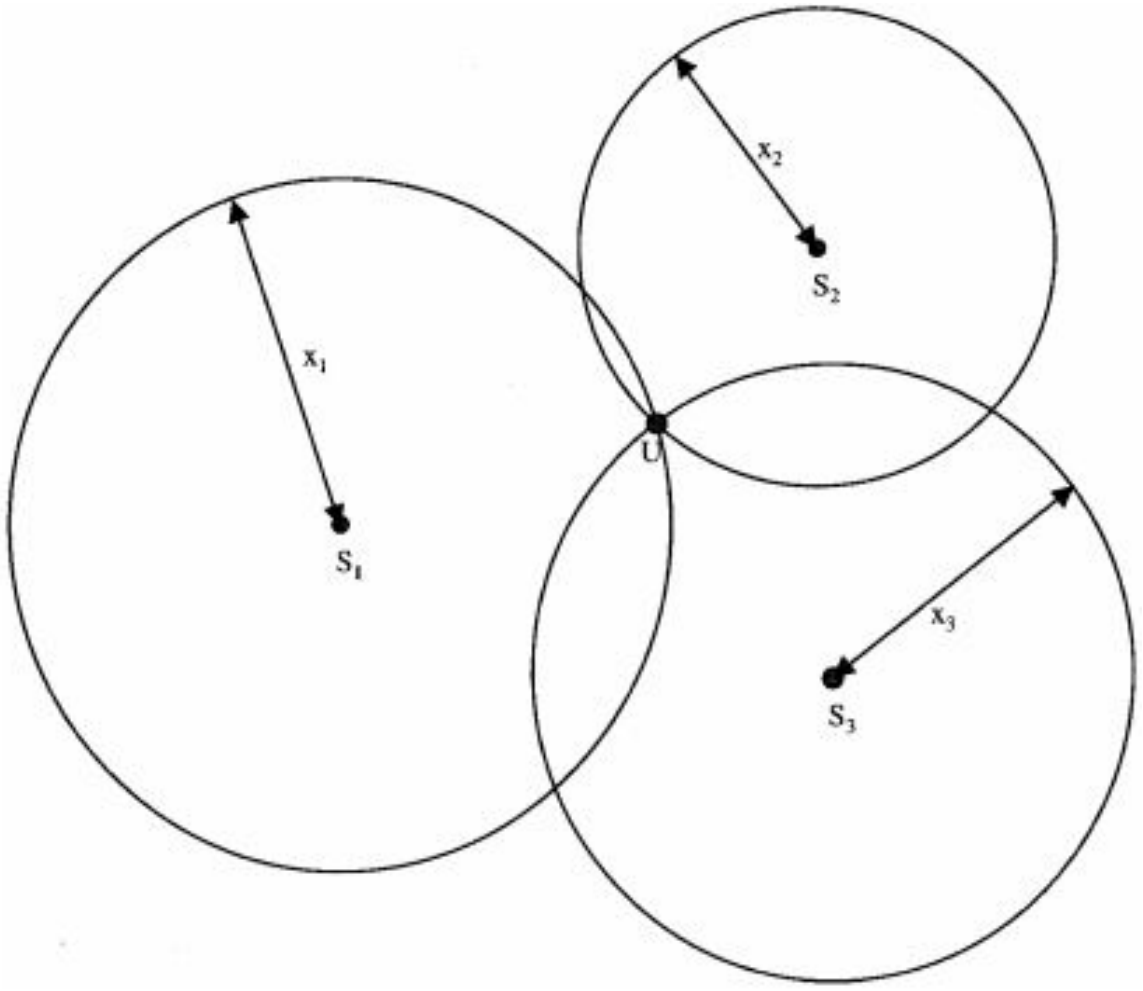

Figure 1.1: A diagram describing the basic process for use of multilateration to determine receiver position from [40].

Unfortunately, this process is only valid if the time synchronization between all of the satellites and the receiver is very precise. Because the time delay is being multiplied by the speed of light, even a very small error in time can result in significant errors in position. The satellites use atomic clocks, which have the precision capabilities necessary to remain synchronized almost exactly, but this technology is too expensive to feasibly deploy in every GPS receiver. Therefore, the error caused by the lack of precision in the receiver clock needs to be accounted for in the calculations.

This is done by computing a pseudorange from the receiver to each satellite. A pseudorange is the combination of the actual distance from the satellite to the receiver and the additional calculated distance due to the time delay in the receiver clock. This can be represented symbolically as seen in equation 1.2:

$$\rho_i = c((t_u + b_{ut}) - t_{si}) \tag{1.2}$$

where ρ_i is the pseudorange from the receiver to satellite i and b_{ut} is the clock bias error caused by the receiver.

Thus, a system of equations of pseudoranges to different satellites can be compiled as seen in equation 1.3:

$$\begin{cases} \rho_1 = \sqrt{(x_1 - x_u)^2 + (y_1 - y_u)^2 + (z_1 - z_u)^2} + b_u \\ \rho_2 = \sqrt{(x_2 - x_u)^2 + (y_2 - y_u)^2 + (z_2 - z_u)^2} + b_u \\ \rho_3 = \sqrt{(x_3 - x_u)^2 + (y_3 - y_u)^2 + (z_3 - z_u)^2} + b_u \\ \rho_4 = \sqrt{(x_4 - x_u)^2 + (y_4 - y_u)^2 + (z_4 - z_u)^2} + b_u \end{cases} \tag{1.3}$$

where x_i, y_i, and z_i are the x, y, and z coordinates of satellite i respectively, x_u, y_u, and z_u are the x, y, and z coordinates of the receiver respectively, and b_u is the error in distance calculated due to the time offset in the receiver clock.

As can be seen from equation 1.3, in order to account for the error due to the time offset now four satellites are required instead of just three as displayed in figure 1.1. However, if at least four satellites are visible to the receiver, equation 1.3 can be solved iteratively to find the values of x_u, y_u, z_u, and b_u. This results in the receiver not only being able to determine its exact location, but also to determine the error in its clock, which can then be neutralized in time synchronization applications.

1.3 GPS Attacks

There are two main types of attacks on GPS receivers: jamming and spoofing. Jamming is the simpler of the two forms, simply involving transmitting noise over GPS frequencies in order to disrupt legitimate signals. This prevents the receiver from calculating its position. Jamming is well understood in the literature [17],[27], and has also been demonstrated numerous times in the real world [26],[2]. Luckily, jamming attacks are typically easy to detect. On the other hand, a spoofing attack is the process in which an adversary generates and transmits a fake signal in order to fool GPS receivers. As the attacker can force the receiver to believe it is in a different location than it really is, spoofing can allow the attacker to lead the victim off course. Multiple reports have discussed the dangers of this form of attack, which can include severe consequences such as steering planes into mountains or ships into hijacking traps [10],[16].

GPS spoofing has already been demonstrated in real world scenarios. In one demonstration, researchers were able to successfully spoof a yacht at sea and steer it off course [3],[9]. Even more concernedly, it is believed that in 2011 Iran was able to spoof the GPS in a CIA stealth drone, fooling it into landing in a spot where they could capture it in order to reverse engineer the technology [34]. These and other such incidents [15],[36],[20] demonstrate the pressing need for security solutions for GPS navigation.

The first step in combating spoofing is detection, which has received substantial attention in the past decade. A literature review of some of the reported results is included in section 1.4. However, even if spoofing can be detected, there is currently not much that can be done about it. There is no way to regain the true signal, and very little research has been reported on locating the attacker. For airborne attackers Jansen and coauthors use crowdsourcing in air planes to localize an attacker [18], which is further improved by [22]. However, this approach relies on dedicated infrastructure, i.e., the OpenSky Network [5], which includes over 700 air traffic communication sensors located all around the world. Such infrastructure unfortunately does not exist for other GPS applications, such as cars.

Yu et al. also attempts to localize an attacker, by using a network of GPS receivers of fixed location, which are typically used for time synchronization in the power grid [41]. However, once again this requires a network of GPS receivers with known locations. In the case of a power grid the receivers are fixed in position, so this is a valid assumption. However, for moving vehicles this

method would no longer be applicable.

This paper proposes to localize spoofing attackers on vehicular GPS by correlating Doppler measurements from multiple vehicles connected with vehicle-to-vehicle communications. Given that vehicle-to-vehicle communication radios are commercially available and commercial GPS receivers have the capability to measure incoming signals' frequencies (see table 1.1 for some examples), the approach does not require dedicated hardware. Both numerical simulations and hardware tests are performed to confirm the effectiveness of the proposed approach.

Table 1.1: Commercial GPS receivers reporting Doppler shift

Brand	**Device**	**Cost**
U-blox	NEO-M8T	$75 [4]
SkyTraq	NS-RAW	$70 [7]
NVS	RasPiGNSS	$170 [12]
Swift	Piksi Multi GNSS Module	$595 [8]
NovAtel	OEM625S	unknown

1.4 Literature Review on Detection of GPS Spoofing

Numerous approaches have been proposed to detect GPS spoofing [30]. One approach to thwart GPS spoofing is to use cryptograph. For example, a navigation message authentication (NMA) based approach is proposed in [35],[29]. In NMA, the navigation message is encrypted or digitally signed with the intent that a receiver can use this information to observe the origin of the signal it is receiving. Other cryptographic defense approaches such as hidden markers [21] have also been examined. Unfortunately, cryptographic defenses have a few major disadvantages. First, these defenses are still vulnerable to replay attacks, where the attacker records a legitimate signal and broadcasts it with a delay [28],[1]. More importantly, these methods require changes to the GPS legacy system. Due to the static nature of the GPS infrastructure and the long deployment cycles, making changes to the legacy system would be costly and time consuming, and is therefore unlikely to occur in the near future.

Non-cryptographic approaches have also been reported to secure GPS. One non-cryptographic method requires cross-correlation of the P(Y) code with a secure receiver [23],[11],[31]. A high correlation value between the secure and insecure receivers implies that both are receiving the same

valid signal. Such correlation based detection can also be performed among several cooperative peers [14]. Unfortunately, this method requires additional high-speed sampling devices to receive raw GPS signals on which the correlation can be performed.

Another method for spoofer detection is SPREE [33]. SPREE is a new form of GPS receiver that uses auxiliary peak tracking to check for similar signals. Since real signals still exist in the presence of a spoofing attack (they are simply overshadowed by the more powerful spoofing signals), the presence of two signals of differing power but similar peaks would indicate the presence of both an authentic signal and a spoofed signal. This would alert the receiver to the presence of a spoofing attack. While this method is quite powerful at detecting attacks, it unfortunately requires hardware upgrades to existing receivers that would be expensive.

Finally, one other option for GPS spoofing detection is to use multiple antennas [39],[19],[25], [37],[38],[32]. If the attacker is spoofing multiple receivers using only one antenna, all receivers will be spoofed to the same location, which would indicate the presence of an attacker. Even if the attacker uses multiple antennas, having multiple receiving antennas still greatly limits the possible locations from which the attacker can successfully operate, which makes spoofing significantly more difficult. However, this method relies on having multiple receivers with known and fixed relative distances, which is not always feasible.

In summary, while there are several methods available for detecting spoofing, they all tend to require either hardware upgrades or alterations to the legacy GPS system which limits their widespread applications to commercial GPS navigation receivers.

Chapter 2

Models and Approach

2.1 Attacker Model

This paper considers an attacker transmitting spoofing signals using an omnidirectional antenna. In this case if multiple targets are spoofed they will lock on the same spoofing signal and report the same location. Thus, if multiple vehicles in a network begin reporting the exact same location, that would indicate the presence of a spoofing attack. Once spoofing is detected, attempts to localize the attacker can begin.

This paper considers two main cases: a stationary attacker and a moving attacker. Note that most of existing results consider stationary attackers. We also consider moving attackers where the attacker can place its transmitter in, e.g., a moving vehicle.

In both the stationary attacker case and the moving attacker case the attacker is assumed able to vary the frequency at which it transmits fake GPS signals. In order to transmit a valid GPS signal the attacker must transmit at a frequency within a few hundred Hertz of the standard satellite transmission (roughly 1575.42 MHz) [40]. However, within this range the attacker is assumed to have full control of the frequency at which they can transmit, including the ability to change frequencies in real time.

2.2 Victim Model

This paper considers a set of moving receivers located on different vehicles. These vehicles travel on the same road and can communicate with each other using vehicle-to-vehicle communications. Each vehicle can record the frequency of the incoming GPS signal, which is reported by most commercial GPS receivers. Each vehicle also has full knowledge of the speed at which it is going and the distance it has traveled between consecutive measurements of the signal frequency. This is reasonable as a vehicle can get the distance information from its odometer. We do not assume that a vehicle knows its exact location.

Each vehicle uses a standard commercial GPS receiver, which reports incoming signal frequencies. Most existing commercial GPS receivers report such measurements. Note that due to the loss of synchronization between receiver clocks and the genuine GPS clocks, these measurements could be subject to errors. We circumvent such errors by using the relative difference between two consecutive measurements in the computation, as will be detailed in section 2.3.

2.3 Approach

2.3.1 Static Spoofer Case

Figure 2.1 shows a schematic of our setup in which we consider $n = 2$ vehicular GPS receivers for the simplicity of exposition. Each receiver takes frequency measurements at m different positions, where m is a positive integer. The receivers will experience some Doppler shift with the signal transmitted from the attacker because of the relative speed between them. Thus, the frequency measured at each point by a given receiver i can be described by the following equation:

$$f = \left(\frac{c + V_i}{c}\right) f_s + \epsilon \tag{2.1}$$

where f is the measured frequency, f_s is the frequency at which the spoofer transmits signals, V_r is the line of sight velocity of the receiver with respect to the spoofer, c is the speed of light, and ϵ is the error in the receiver. ϵ is caused by the difference in the clocks between the receiver and the GPS satellites. It can be eliminated by considering the difference between different samples. Although some error will still occur from oscillator drift, over short sampling times this will tend to

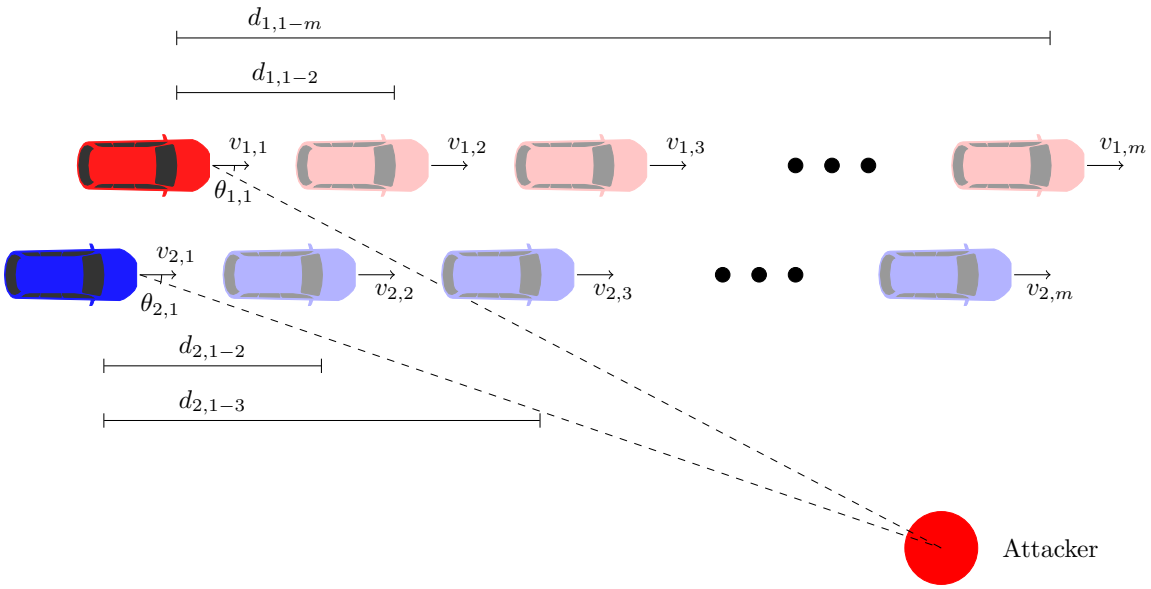

Figure 2.1: A diagram of the receivers and the attacker. There are two receivers, 1 and 2, each of which takes measurements at m different instances of measuring time. Each receiver has knowledge of the speed it is moving at each time as well as the distance it has traveled since the first measurement.

be minimal [13]. For instance, the difference in frequency in receiver i between the first measurement and the jth measurement, where j is some integer between 2 and n, can be represented as follows:

$$\Delta f_{i,1-j} = f_{i,1} - f_{i,j} = \left(\frac{c + V_{i,1}}{c}\right) f_{s,1} - \left(\frac{c + V_{i,j}}{c}\right) f_{s,j} \tag{2.2}$$

As we do not assume that the spoofer is using a constant frequency in signal transmission, we used $f_{s,1}$ and $f_{s,j}$ to denote the respective frequencies at which the spoofing is transmitting when the first and jth measurements were conducted. This equation can be simplified as follows:

$$\Delta f_{i,1-j} = \frac{1}{c}\left(f_{s,1}V_{1,1} - f_{s,j}V_{i,j}\right) + f_{s,1} - f_{s,j} \tag{2.3}$$

The line of sight velocity of receiver i at time j with respect to the attacker is unknown and can be represented as:

$$V_{i,j} = v_{i,j}\cos(\theta_{i,j}) \tag{2.4}$$

where $v_{i,j}$ is the speed of receiver i at time j and $\theta_{i,j}$ is the angle between receiver velocity and its direction with respect to the attacker, as illustrated in figure 2.1. Combining equations (2.3) and

(2.4) leads to:

$$\Delta f_{i,1-j} = \frac{1}{c}\left(f_{s,1} v_{1,1}\cos(\theta_{1,1}) - f_{s,j} v_{i,j}\cos(\theta_{i,j})\right) + f_{s,1} - f_{s,j} \tag{2.5}$$

Furthermore, based on the geometry of the formation, $\cos(\theta_{i,j})$ can be represented in terms of variables referencing receiver 1 at the first time sample, described below:

$$\cos(\theta_{i,j}) = \frac{r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j}}{\sqrt{(r_{i,1}\sin(\theta_{i,1}))^2 + (r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j})^2}} \tag{2.6}$$

where $r_{i,1}$ is the distance from receiver i to the attacker when the first measurement was conducted, and $d_{i,1-i}$ is the distance between receiver i's first and jth measurements. This relationship can then be substituted into equation (2.5), resulting in the following equation:

$$\Delta f_{i,1-j} = f_{s,1} - f_{s,j} + \frac{1}{c} f_{s,1} v_{i,1}\cos(\theta_{i,1}) - \frac{1}{c}\left(\frac{f_{s,1} v_{i,j}(r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j})}{\sqrt{(r_{i,1}\sin(\theta_{i,1}))^2 + (r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j})^2}}\right) \tag{2.7}$$

Equation (2.7) can be further rewritten as:

$$\Delta f_{i,1-j} = f_{s,1} - f_{s,j} + \frac{1}{c}\left(f_{s,1} v_{i,1}\cos(\theta_{i,1}) - \frac{f_{s,1} v_{i,j}(r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j})}{\sqrt{r_{i,1}^2 + d_{i,1-j}^2 - 2 r_{i,1} d_{i,1-j}\cos(\theta_{i,1})}}\right) \tag{2.8}$$

Representing $\cos(\theta_{i,1})$ with x, equation (2.8) can be simplified to the following:

$$\Delta f_{i,1-j} = f_{s,1} - f_{s,j} + \frac{1}{c}\left(f_{s,1} v_{i,1} x - \frac{f_{s,1} v_{i,j}(r_{i,1} x - d_{i,1-j})}{\sqrt{r_{i,1}^2 + d_{i,1-j}^2 - 2 r_{i,1} d_{i,1-j} x}}\right) \tag{2.9}$$

This same method can be used for every measurement point made by receiver 1, as well as for all other receivers. This ultimately results in the following system of equations:

$$
\begin{cases}
\Delta f_{1,1-2} = f_{s,1} - f_{s,2} + \frac{1}{c}\left(f_{s,1}v_{1,1}x - \frac{f_{s,1}v_{1,2}(r_{1,1}x - d_{1,1-2})}{\sqrt{r_{1,t}^2 + d_{1,1-2}^2 - 2r_{1,1}d_{1,1-2}x}}\right) \\
\Delta f_{1,1-3} = f_{s,1} - f_{s,3} + \frac{1}{c}\left(f_{s,1}v_{1,1}x - \frac{f_{s,1}v_{1,3}(r_{1,1}x - d_{1,1-3})}{\sqrt{r_{1,t}^2 + d_{1,1-3}^2 - 2r_{1,1}d_{1,1-3}x}}\right) \\
\vdots \\
\Delta f_{1,1-m} = f_{s,1} - f_{s,m} + \frac{1}{c}\left(f_{s,1}v_{1,1}x - \frac{f_{s,1}v_{1,m}(r_{1,1}x - d_{1,1-m})}{\sqrt{r_{1,1}^2 + d_{1,1-m}^2 - 2r_{1,1}d_{1,1-m}x}}\right) \\
\Delta f_{2,1-2} = f_{s,1} - f_{s,2} + \frac{1}{c}\left(f_{s,1}v_{2,1}x - \frac{f_{s,1}v_{2,2}(r_{2,1}x - d_{2,1-2})}{\sqrt{r_{2,1}^2 + d_{2,1-2}^2 - 2r_{2,1}d_{2,1-2}x}}\right) \\
\vdots \\
\Delta f_{2,1-m} = f_{s,1} - f_{s,m} + \frac{1}{c}\left(f_{s,1}v_{2,1}x - \frac{f_{s,1}v_{2,m}(r_{2,1}x - d_{2,1-m})}{\sqrt{r_{2,1}^2 + d_{2,1-m}^2 - 2r_{2,1}d_{2,1-m}x}}\right) \\
\vdots \\
\Delta f_{n,1-2} = f_{s,1} - f_{s,2} + \frac{1}{c}\left(f_{s,1}v_{n,1}x - \frac{f_{s,1}v_{n,2}(r_{n,1}x - d_{n,1})}{\sqrt{r_{n,1}^2 + d_{n,1-2}^2 - 2r_{n,1}d_{n,1-2}x}}\right) \\
\vdots \\
\Delta f_{n,1-m} = f_{s,1} - f_{s,m} + \frac{1}{c}\left(f_{s,1}v_{n,1}x - \frac{f_{s,1}v_{n,m}(r_{n,1}x - d_{n,1})}{\sqrt{r_{n,1}^2 + d_{n,1-m}^2 - 2r_{n,1}d_{n,1-m}x}}\right)
\end{cases}
\tag{2.10}
$$

Suppose there are n receivers, each conducting m measurements, then $n(m-1)$ equations in (2.10) can be constructed. In these equations, there are $2n+m$ unknowns, ie. θ for each receiver, r for each receiver, and f_s transmitted at each time instance. Therefore, when m is larger than 6, we have $n(m+1) > 2n+m$, and hence can solve for the unknowns in (2.10). Using the same argument, we can know that three receivers only require five measurements per receivers and four or more receivers only require four measurements per receiver. However, any number of receivers can take additional measurements per receiver to potentially improve accuracy. As such, once this system of equations is solved, the position of the attacker is known relative to each receiver. Note that since the cosine of an angle can correspond to two different angles, there are two possible solutions. Due to the symmetry of the problem, it is impossible to narrow it down to only one solution, so both locations would have to be investigated to localize the attacker.

The above approach to calculating $r_{i,1}$ and $\theta_{i,1}$ hence obtaining the location of the spoofer is applicable only when the measurements are noise-free. Given that the measurements are always sub-

ject to noise, we choose to estimate the location of the spoofer by solving the following optimization problem:

$$\begin{aligned} &\min_{X\in\mathbb{R}^d} \sum_{i=1}^{n}\sum_{j=2}^{m} E_{i,j}^2 \\ &X = (\theta_{1,1}, \theta_{2,1}, ..., \theta_{i,1}, r_{1,1}, ..., r_{i,1}, f_{s,1}, ..., f_{s,j}) \end{aligned} \tag{2.11}$$

where $E_{i,j}$ is the error for car i at sample j, which is the difference between the measure Doppler shift and the Doppler shift calculated based on the chosen parameters or:

$$E_{i,j} = \Delta f_{i,1-j} - f_{s,1} - f_{s,j} + \frac{1}{c}\left(f_{s,1}v_{i,1}x - \frac{f_{s,1}v_{i,j}(r_{i,1}x - d_{i,1-j})}{\sqrt{r_{i,1}^2 + d_{i,1-j}^2 - 2r_{i,1}d_{i,1-j}x}}\right) \tag{2.12}$$

Solving for (2.11) gives the optimal solution for this problem.

2.3.2 Mobile Spoofer Case

Just like in the stationary spoofer case, in the moving spoofer the position of an attacker can also be calculated by examining the difference between Doppler shifts at different measurement points. However, in this case the Doppler shift is not only affected by the motion of the receivers but also by the unknown motion of the attacker. Therefore, the difference in Doppler shifts between two measurement points can be characterized by the following equation for receiver i:

$$\Delta f_{i,1-j} = f_{s,1} - f_{s,j} + \frac{1}{c}\left(f_{s,1}(V_{i,1} + V_{s,1}) - f_{s,j}(V_{i,j} + V_{s,j})\right) \tag{2.13}$$

where $V_{i,1}$ and $V_{i,j}$ are the line of sight velocities of the victim with respect to the spoofer when conducting the first and jth measurements respectively and $V_{s,1}$ and $V_{s,j}$ are the line of sight velocities of the spoofer when the first and jth measurement were conducted by receiver i, respectively.

Just like in the stationary spoofer case, the line of sight velocities are not known. So it is represented as follows:

$$V_{i,j} = v_{i,j}\cos(\theta_{i,j}) \tag{2.14}$$

where $v_{i,j}$ is the magnitude of the velocity of the victim, which is known to vehicle i, and $\theta_{i,j}$ is the

angle that vehicle i's velocity makes with the direction to the spoofer.

All line of sight victim velocities at future times can also be represented in terms of $\theta_{i,1}$. Based on the geometry of the problem, $\cos(\theta_{i,j})$ can be represented as follows:

$$\cos(\theta_{i,j}) = \frac{r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j} + T * v_s \cos(\theta_s)}{\sqrt{r_{y,i,j}^2 + r_{x,i,j}^2}} \tag{2.15}$$

where

$$r_{y,i,j} = r_{i,1}\cos(\theta_{i,1}) - d_{i,1-j} + (i-1)T * v_s \cos(\theta_s) \tag{2.16}$$

and

$$r_{x,i,j} = r_{i,1}\sin(\theta_{i,1}) + (i-1)T * v_s \sin(\theta_s) \tag{2.17}$$

Here, T is the sampling period of the receiver.

In order to represent the attack motion's influence on the measured Doppler shift a similar process can be completed. Once again, the velocity of the spoofer can be multiplied by the cosine of the angle it makes with the receiver. However, since the angle the attacker's velocity makes with each victim is constantly changing, it cannot be represented as a single variable and must therefore be defined by multiple other variables for each time instant. For instance, the angle that the velocity of the spoofer makes with receiver i at the jth time instant can be represented as:

$$\theta_{s,i,j} = \theta_s + 180 - \theta_{i,j} \tag{2.18}$$

where $\theta_{s,i,j}$ is the angle that the spoofer's velocity makes with receiver i at time j and θ_s is the angle the attacker's velocity makes with the vertical axis, which is assumed to be the same during vehicle i's m samples.

Furthermore, the angle the velocity of the spoofer makes with receiver i at other time instants can be represented in terms of variables from the first time instant, as can be seen below for the jth time sample:

$$\theta_{s,i,j} = \theta_s + 180 - \cos^{-1}(\cos(\theta_{i,j})) \tag{2.19}$$

where $\cos(\theta_{i,j})$ can be represented as demonstrated in equation (2.15).

Therefore, equations (2.14) through (2.19) can be substituted into equation (2.13) to produce

the following equation:

$$\Delta f_{i,1-j} = f_{s,1} - f_{s,j} + \frac{1}{c}(f_{s,1}(v_{i,1}cos(\theta_{i,1}) + v_s \cos(\theta_s + 180 - \theta_{i,j})) - f_{s,j} * (v_{i,j} \cos(\theta_{i,1}) + v_s \cos(\theta_s + 180 - \cos^{-1}(cos(\theta_{i,j}))))) \quad (2.20)$$

A similar equation can be created for each receiver at each sample after the first. This

results in the following system of equations:

$$
\begin{cases}
\Delta f_{1,1-2} = f_{s,1} - f_{s,2} + \\
\frac{1}{c}(f_{s,1}(v_{1,1}cos(\theta_{1,1}) + v_s\cos(\theta_s + 180 - \theta_{1,1})) - f_{s,2} \\
*(v_{1,2}\cos(\theta_{1,1}) + v_s\cos(\theta_s + 180 - \cos^{-1}(cos(\theta_{1,2}))))) \\
\\
\Delta f_{1,1-3} = f_{s,1} - f_{s,3} + \\
\frac{1}{c}(f_{s,1}(v_{1,1}cos(\theta_{1,1}) + v_s\cos(\theta_s + 180 - \theta_{1,1})) - f_{s,3} * \\
(v_{1,3}\cos(\theta_{1,1}) + v_s\cos(\theta_s + 180 - \cos^{-1}(cos(\theta_{1,3}))))) \\
\vdots \\
\Delta f_{1,1-m} = f_{s,1} - f_{s,m} + \\
\frac{1}{c}(f_{s,1}(v_{1,1}cos(\theta_{1,1}) + v_s\cos(\theta_s + 180 - \theta_{1,1})) - f_{s,m} * \\
(v_{1,m}\cos(\theta_{1,1}) + v_s\cos(\theta_s + 180 - \cos^{-1}(cos(\theta_{1,m}))))) \\
\\
\Delta f_{2,1-2} = f_{s,1} - f_{s,2} + \\
\frac{1}{c}(f_{s,1}(v_{2,1}cos(\theta_{2,1}) + v_s\cos(\theta_s + 180 - \theta_{2,1})) - f_{s,2} * \\
(v_{2,2}\cos(\theta_{2,1}) + v_s\cos(\theta_s + 180 - \cos^{-1}(cos(\theta_{2,2}))))) \\
\vdots \\
\Delta f_{2,1-m} = f_{s,1} - f_{s,m} + \\
\frac{1}{c}(f_{s,1}(v_{2,1}cos(\theta_{2,1}) + v_s\cos(\theta_s + 180 - \theta_{2,1})) - f_{s,m} * \\
(v_{2,m}\cos(\theta_{2,1}) + v_s\cos(\theta_s + 180 - \cos^{-1}(cos(\theta_{2,m}))))) \\
\vdots \\
\Delta f_{n,1-2} = f_{s,1} - f_{s,2} + \\
\frac{1}{c}(f_{s,1}(v_{n,1}cos(\theta_{n,1}) + v_s\cos(\theta_s + 180 - \theta_{n,1})) - f_{s,2} * \\
(v_{n,2}\cos(\theta_{n,1}) + v_s\cos(\theta_s + 180 - \cos^{-1}(cos(\theta_{n,2}))))) \\
\vdots \\
\Delta f_{n,1-m} = f_{s,1} - f_{s,m} + \\
\frac{1}{c}(f_{s,1}(v_{n,1}cos(\theta_{n,1}) + v_s\cos(\theta_s + 180 - \theta_{n,1})) - f_{s,m} * \\
(v_{n,m}\cos(\theta_{n,1}) + v_s\cos(\theta_s + 180 - \cos^{-1}(cos(\theta_{n,m})))))
\end{cases}
\tag{2.21}
$$

Once again, suppose there are n receivers, each conducting m measurements. This allows for

the construction of $n(m-1)$ equations in (2.21). In these equations there are $2n+m+2$ unknowns, which once again include θ for each receiver, r for each receiver, and the transmitted frequency, f_s, at each time instant. However, in this case the spoofer also has an unknown speed, v_s, and direction, θ_s. Thus, when n is 3 and m is 6, we have $n(m-1) > 2n+m+2$, and can thus solve for the unknowns. Using the same argument, we can say that as the number of receivers increases the number of required measurements decreases. However, any number of receivers can still take additional measurements to potentially improve accuracy. Therefore, once this system is solved, the position of the attacker is known relative to each receiver and the speed and direction of the attacker is also obtained. Note that once again the symmetry of the problem leads to two potential solutions, which would both need to be investigated.

Similarly to the stationary case, noise in the system prevents it from finding an actual solution. Therefore, once again it is necessary to minimize localization error based on the following optimization problem:

$$\begin{aligned} &\min_{X\in\mathbb{R}^d} \sum_{i=1}^{n}\sum_{j=2}^{m} E_{i,j}^2 \\ &X = (\theta_{1,1}, \theta_{2,1}, ..., \theta_{i,1}, r_{1,1}, ..., r_{i,1}, f_{s,1}, ..., f_{s,j}, v_s, \theta_s) \end{aligned} \tag{2.22}$$

where $E_{i,j}$ is the error between the measured Doppler shift and the Doppler shift calculated based on parameters, as demonstrated below:

$$\begin{aligned} E_{i,j} = \Delta f_{i,1-j} - f_{s,1} - f_{s,j} + \frac{1}{c}(f_{s,1}(v_{i,1}cos(\theta_{i,1}) + v_s\cos(\theta_s + 180 - \theta_{i,1})) - \\ f_{s,j}(v_{i,j}\cos(\theta_{i,1}) + v_s\cos(\theta_s + 180 - \cos^{-1}(cos(\theta_{i,j}))))) \end{aligned} \tag{2.23}$$

Chapter 3

Evaluation Based on Numerical Simulations

3.1 Simulation Setup

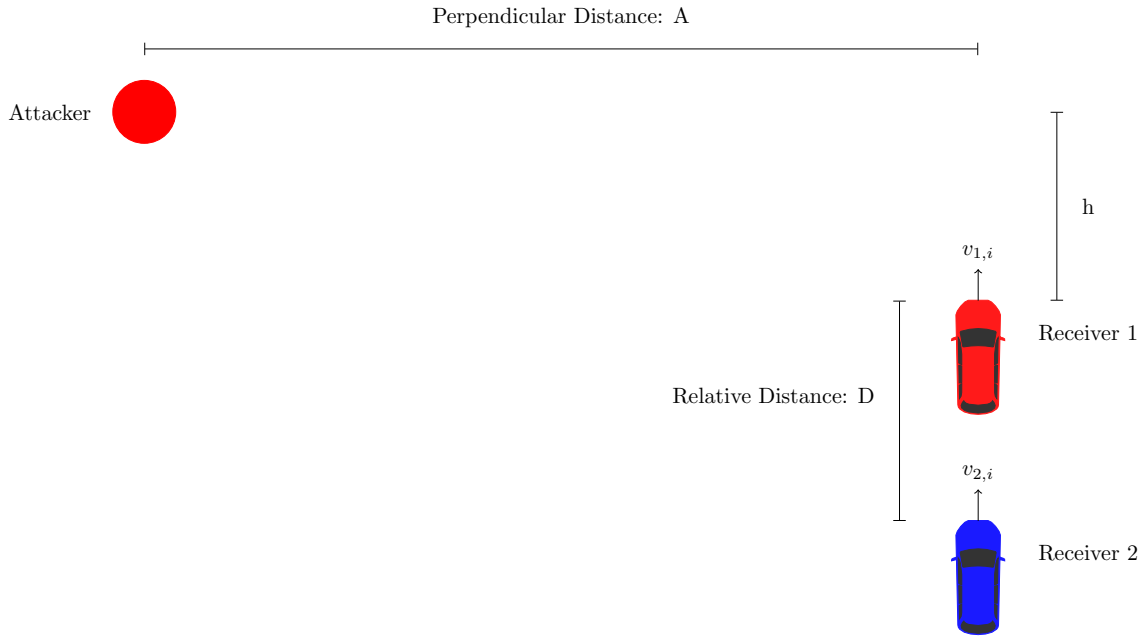

Figure 3.1: A diagram of the spoofer setup used in numerical simulations.

Numerical simulations were first conducted to verify the effectiveness of our attack localization approach.

In the simulation it is assumed that all vehicles travel along the same road with the same constant speed, ie. $v_{1,j} = v_{2,j}$, 20 m/s, as illustrated in figure 3.1. This setting involves three parameters, the relative distances between consecutive receivers (D), the perpendicular distance from the attacker to the receivers (A), and the parallel distance from the front vehicle to the attacker (h). The influence of these parameters as well as the number of samples/cars on the localization performance were systematically evaluated.

For each simulation, a test was run where the approach outlined in section 2.3 was used to calculate the position of the attacker relative to each receiver. The results of a typical test can be seen in figure 3.2. In this figure, the blue rectangles represent the receivers, which are moving in the positive y-direction, the red circle represents the spoofer, and the blue and light blue circles are the calculated positions of the attacker relative to each receiver.

As can be seen from figure 3.2, each test resulted in two sets of possible locations for the attacker. This is due to the symmetry of the problem and is unavoidable. In a real-world scenario, both sets of calculated positions would need to be investigated, but for the purposes of this analysis only the calculations nearest to the spoofer are examined. The error in each test is said to be the distance from the true position of the spoofer to the calculated position of the spoofer relative to each receiver.

Similar results were gathered in the moving spoofer scenario. Figure 3.3 depicts the results of a standard moving spoofer simulation. Once again, the receivers are represented as blue rectangles and are moving in the positive y-direction. Furthermore, the attacker is still represented as a red circle, although a red circle is included for the attacker position at every time sample. However in this case, the attacker position is calculated relative to the receiver at each position.

Once again, due to the symmetry of the problem this approach will generate two possible sets of solutions. Figure 3.3 only displays one of these solutions for clarity, but either one is equally likely. Once again, for this analysis only the nearest solution was examined, but for practical applications both solutions would have to be considered. The spoofer's position is calculated at the time of each measurement, however for these simulations the analysis focused on error at the first position because once the first position and the speed of the spoofer are known, the spoofer's position at any other time can be calculated trivially.

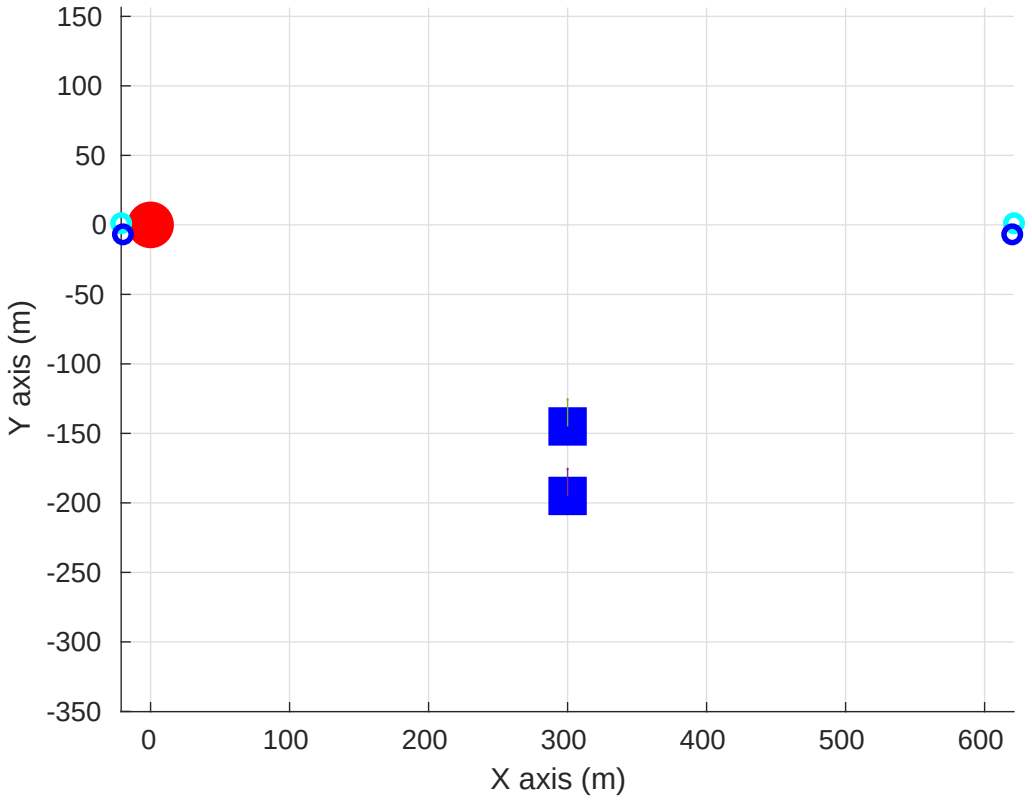

Figure 3.2: Typical simulation results for the stationary spoofer case.

3.2 Influence of Number of Samples

Setting D equal to 10 meters, A equal to 100 meters, and h equal to 145 meters, we first evaluated the performance of the algorithm under different number of samples. To emulate measurement noise Gaussian noise with standard deviation of .05 was added. Three cases were considered, with the number of vehicle receivers set to 2, 3, and 4 respectively. Each vehicle recorded a measurement every three seconds. The errors of localization for the three cases with different numbers of samples are illustrated in figure 3.4. In the figure, we run each test for 100 runs. Note that in the 2-car case no data is given when the number of samples is 5, as in this case the number of samples is not enough to arrive at a solution.

It can be seen that as the number of samples increases the average error consistently decreases. This was expected as additional data should allow for more accurate calculations. Further-

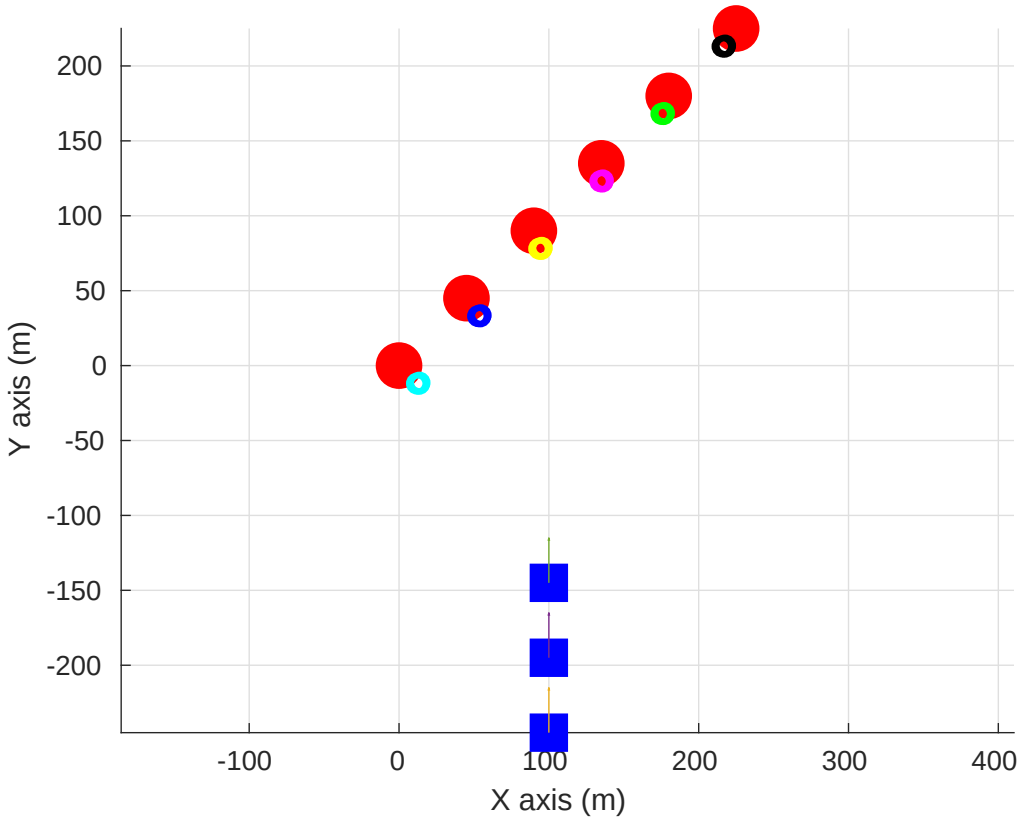

Figure 3.3: Typical simulation results for the moving spoofer case.

more, as the number of vehicles increased the average error also decreased.

Similar simulations were carried out for the mobile spoofer case. Samples were still collected every three seconds by each vehicle and Gaussian noise was assumed to have a standard deviation of .05.

These simulations were conducted for two different formations of moving spoofers: one where the spoofer is moving at a 45 degree angle relative to the receivers (figure 3.5) and one where the spoofer is on the same road as the receivers but traveling in the opposite direction (figure 3.6). In both formations, all victims were assumed to be on the same road driving in the same direction. In figure 3.6 the perpendicular distance, A, is set to 5 meters to reflect the distance to the other side of the road. Furthermore, the spoofer and the receivers are all moving at the same speed, 20 m/s.

Figure 3.7 displays the localization error in the first formation. Once again, it can be seen that the localization becomes more accurate with additional samples and vehicles. A similar

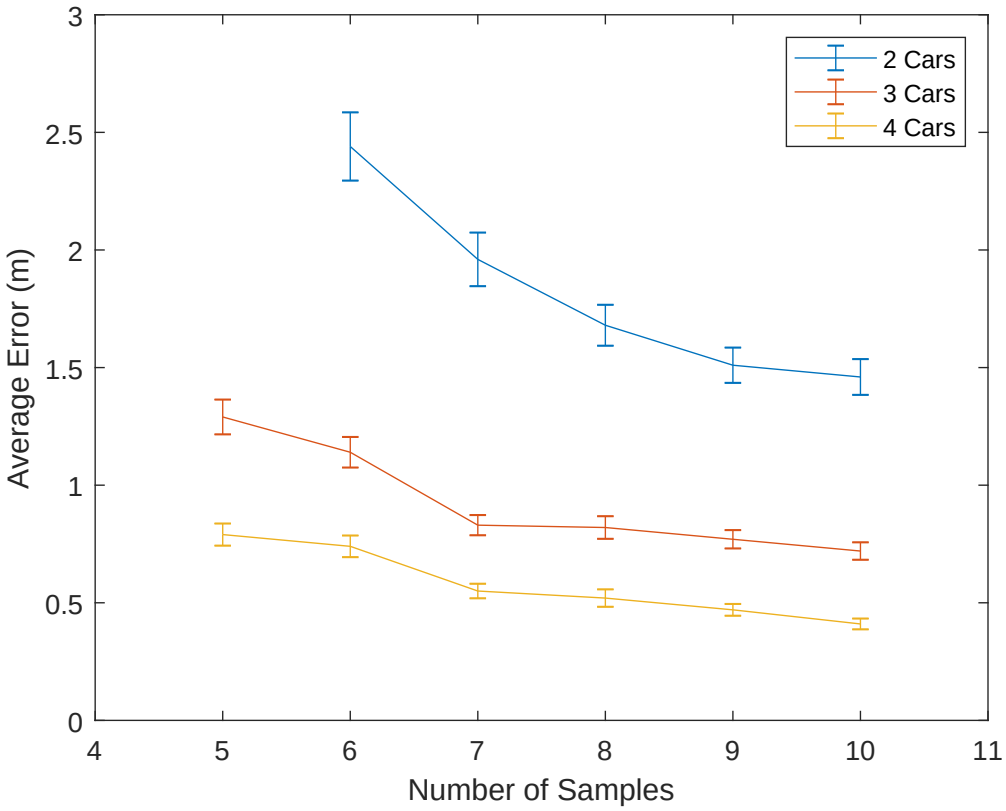

Figure 3.4: The influence of the number of samples (m) on localization performance in the static spoofer case.

simulation was conducted for the second formation, as illustrated in figure 3.8. However, in this case it can be seen that increased numbers of samples had no effect on the localization accuracy. Figure 3.8 shows the results for the three car case, but the four and five car plots are identical, revealing that an increased number of vehicles also has no effect on localization accuracy under these conditions. This is reasonable because the only change in Doppler shift occurs when a vehicle passes the spoofer, so adding additional measurements at other points does not actually lead to additional useful information.

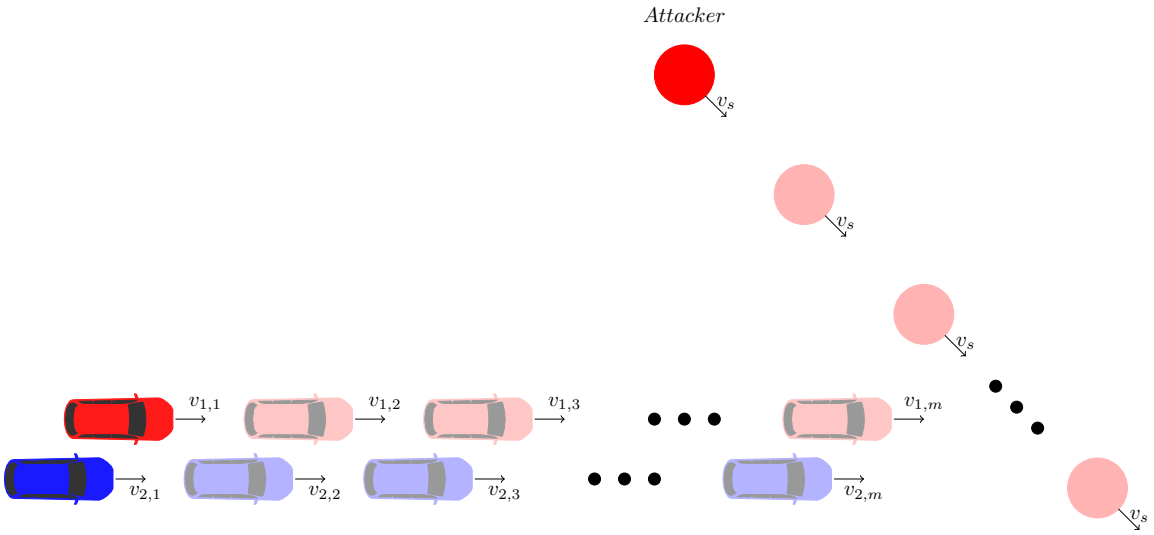

Figure 3.5: A diagram of the formation examined where the attacker moves at a 45 degree angle with the receivers. Only two receivers are shown here due to space constraints.

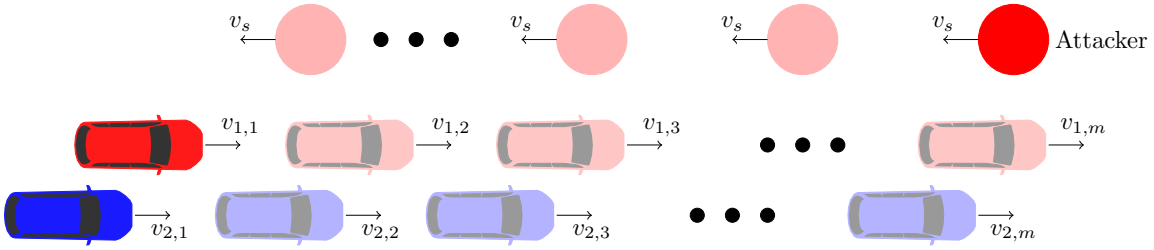

Figure 3.6: A diagram of the formation of the receivers moving in the opposite direction of the attacker on the same road.

3.3 Influence of Parallel Distance, h

We also evaluated the influence of h, the parallel distance from the front vehicle to the attacker, on the localization performance in figure 3.9. As can be seen, the error starts fairly high for low values of h before decreasing, staying relatively constant for some time, and then increasing again. If h continues to increase past the plotted values, the error increases far more dramatically. This trend holds true for different numbers of vehicles and indicates that this method is most accurate when the receivers pass the attacker during conducting measurements. This is to be expected as this will allow for the greatest range in changing Doppler shifts.

The effect of changing h was also evaluated in the moving case illustrated in figure 3.5, as

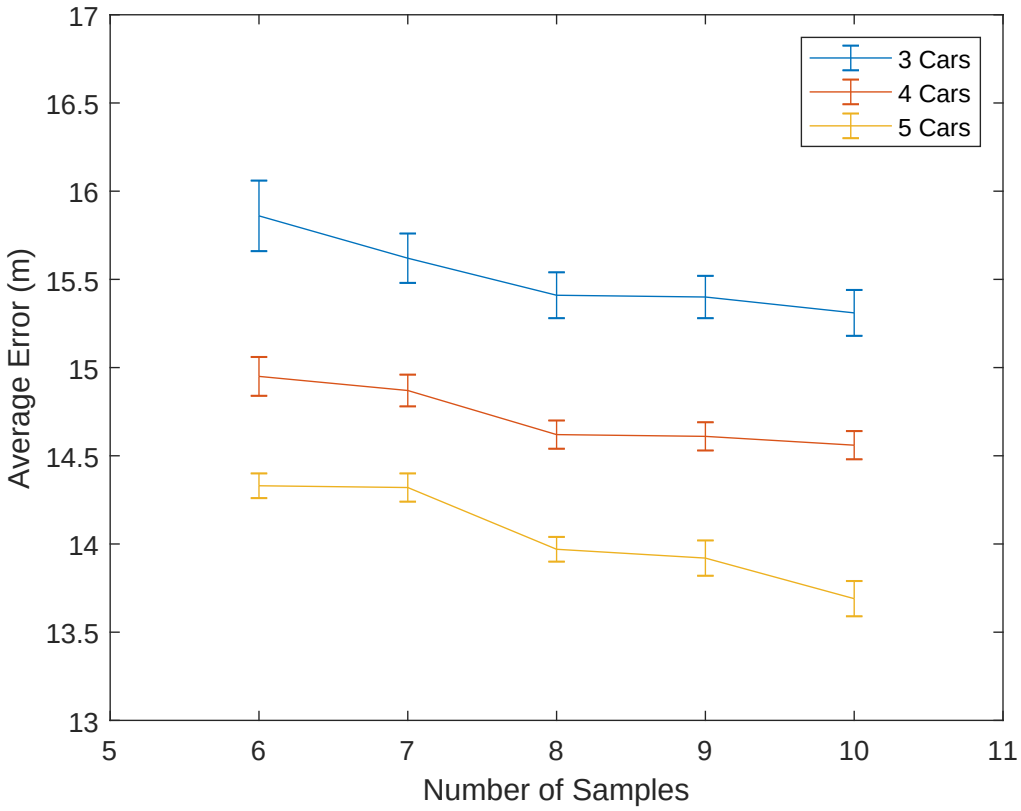

Figure 3.7: The influence of the number of samples (m) on localization performance in the moving spoofer case illustrated in figure 3.5.

can be seen in figure 3.10. Similarly to the stationary spoofer case, the error at first decreases with increasing h and then begins to increase again. Once again, this demonstrates that our method is most effective where the receivers cross the spoofer.

3.4 Influence of Perpendicular Distance, A

The effect of the perpendicular attacker distance, A, was also evaluated for both the stationary and moving spoofer cases. Figure 3.11 displays the effect of A in the stationary case. In general, as A increases so does the calculated error. However, if A is too low, such as when it is equal to 10 meters, the error is also high.

Figure 3.12 demonstrates the effect of changing A in the 45 degree moving attacker case.

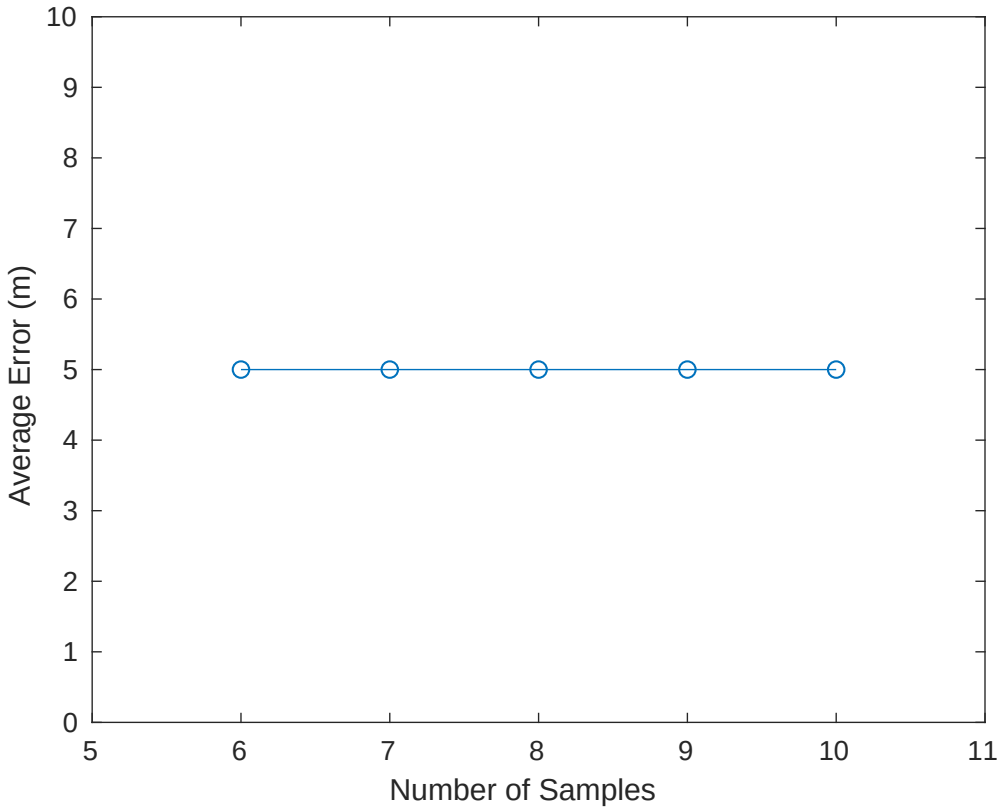

Figure 3.8: The influence of the number of samples (m) on localization performance in the moving spoofer case illustrated in figure 3.6.

Just like in the stationary case, as A increases so does the calculated error.

3.5 Influence of the Relative Vehicle Distance, D

Finally, simulations were conducted to evaluate the influence of D, the relative distance between receivers. Figure 3.13 displays the average error with changing D for the stationary spoofer case. As can be seen, the error generally decreases as D increases, which makes sense because at greater values for D the Doppler shift is more different for different receivers. However, after a distance of 60 meters, the average error increases dramatically, to as much as several hundred meters of error. This is not shown in figure 3.13 as the difference in error will obscure the trends in the first 60 meters. This effect is most pronounced with more receivers due to the fact that with more

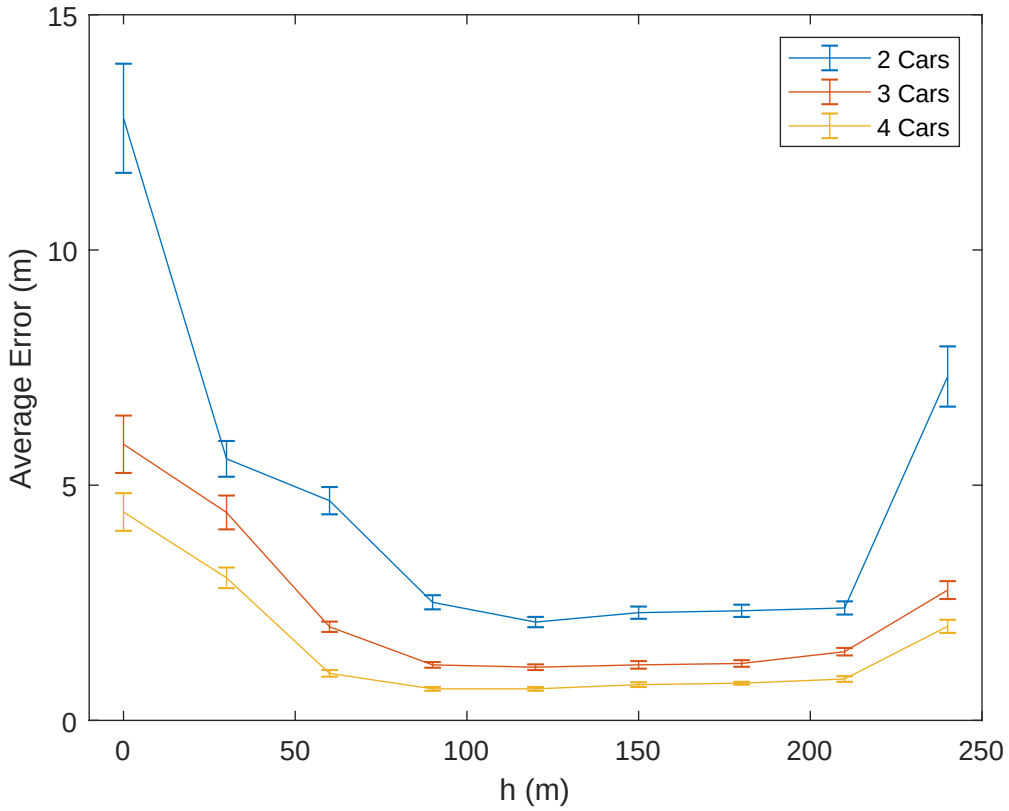

Figure 3.9: The influence of the distance h on the localization performance for the static spoofer case.

receivers the distance from the front receiver to the back receiver is greatly affected by the distance between each receiver. Therefore, once the back receiver gets too far away the method is no longer able to function effectively.

Figure 3.14 displays the effect of changing D in the moving spoofer case illustrated in figure 3.5. Unlike the stationary case, the error in the moving case increases fairly consistently with an increase in D. Thus, the moving spoofer case is most accurate at low relative distances between receivers. This is because the numerical solver used to localize the spoofer in the moving system assumes that $\theta_{i,1}$ is very similar for each receiver. As D increases, this is no longer true, especially with additional receivers, so the solver is no longer able to reach an accurate solution. As such, this method is only effective to localize moving attackers when distances between receivers are small.

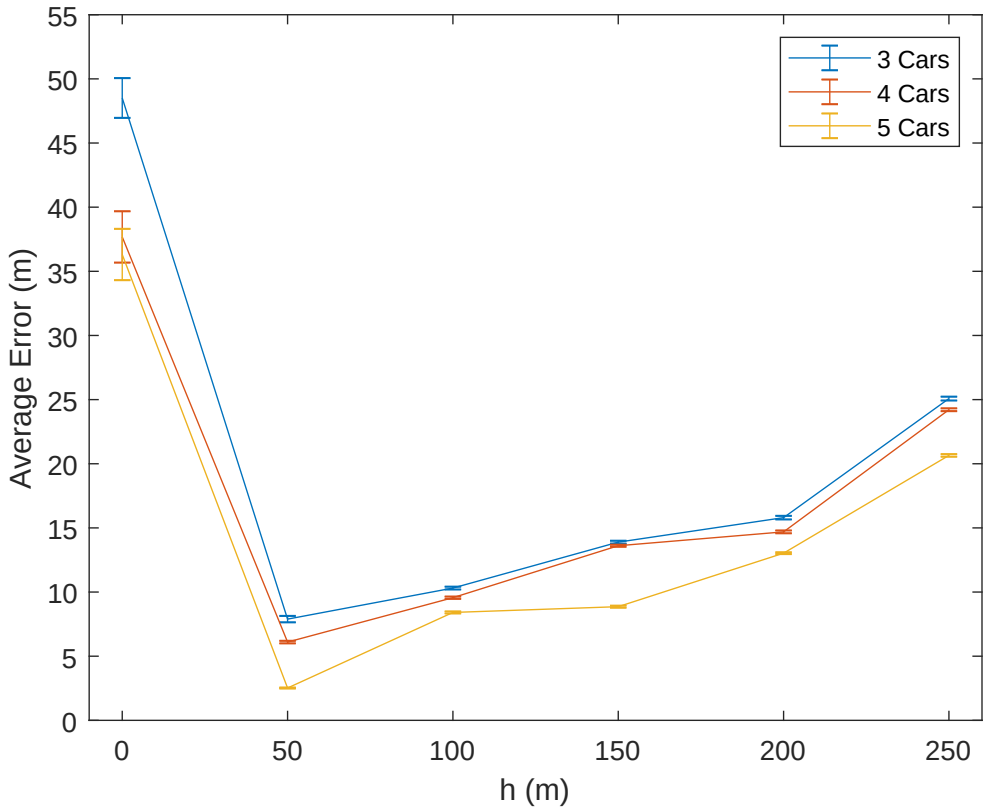

Figure 3.10: The influence of the distance h on the localization performance for the moving spoofer case illustrated in figure 3.5.

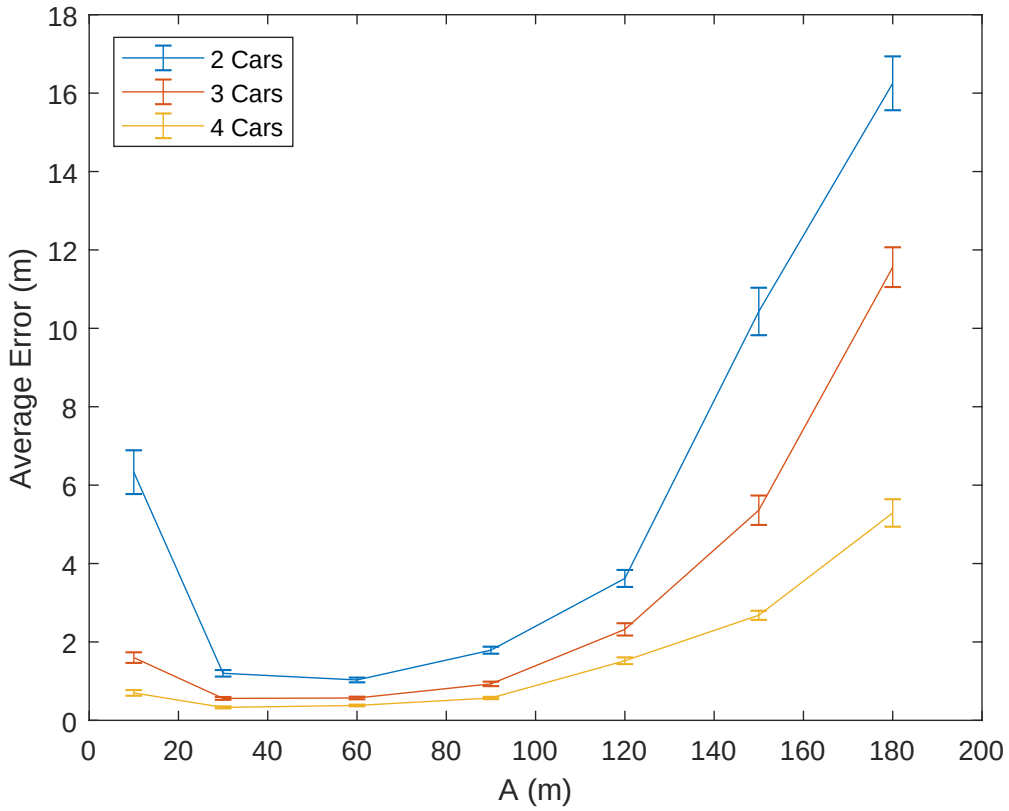

Figure 3.11: The influence of the attacker distance, A, on the localization performance in the static spoofer case.

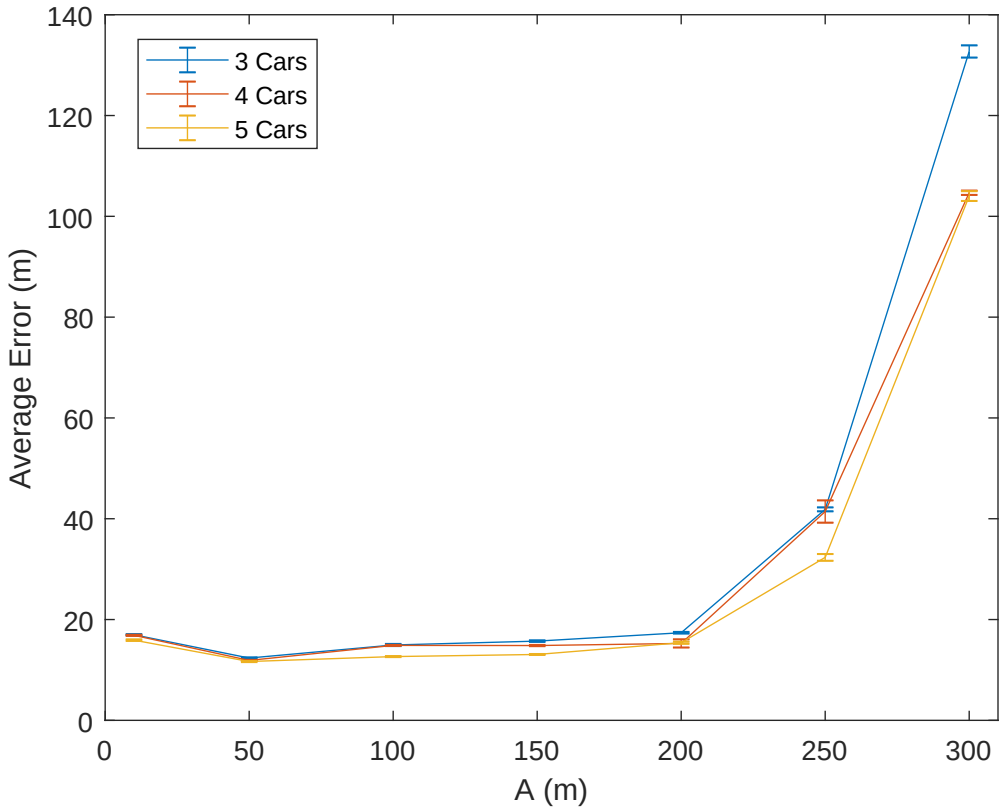

Figure 3.12: The influence of the attacker distance, A, on the localization performance for the moving spoofer case illustrated in figure 3.5.

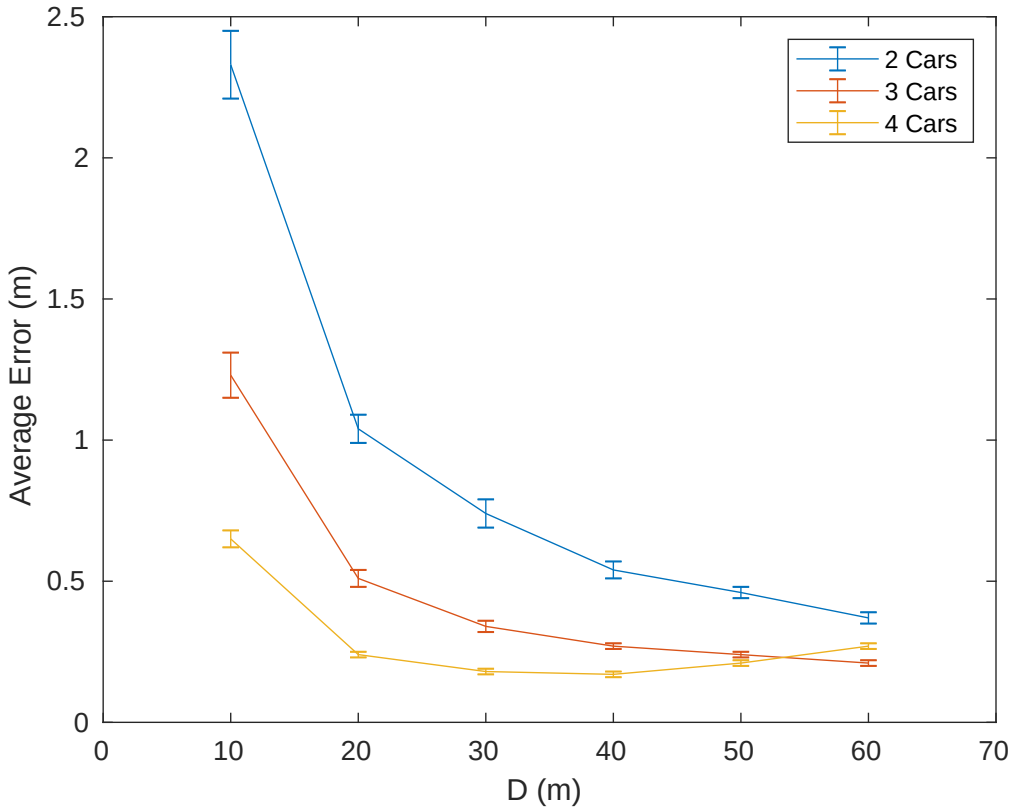

Figure 3.13: The influence of the relative receiver distance, D, on localization performance for the static spoofer case.

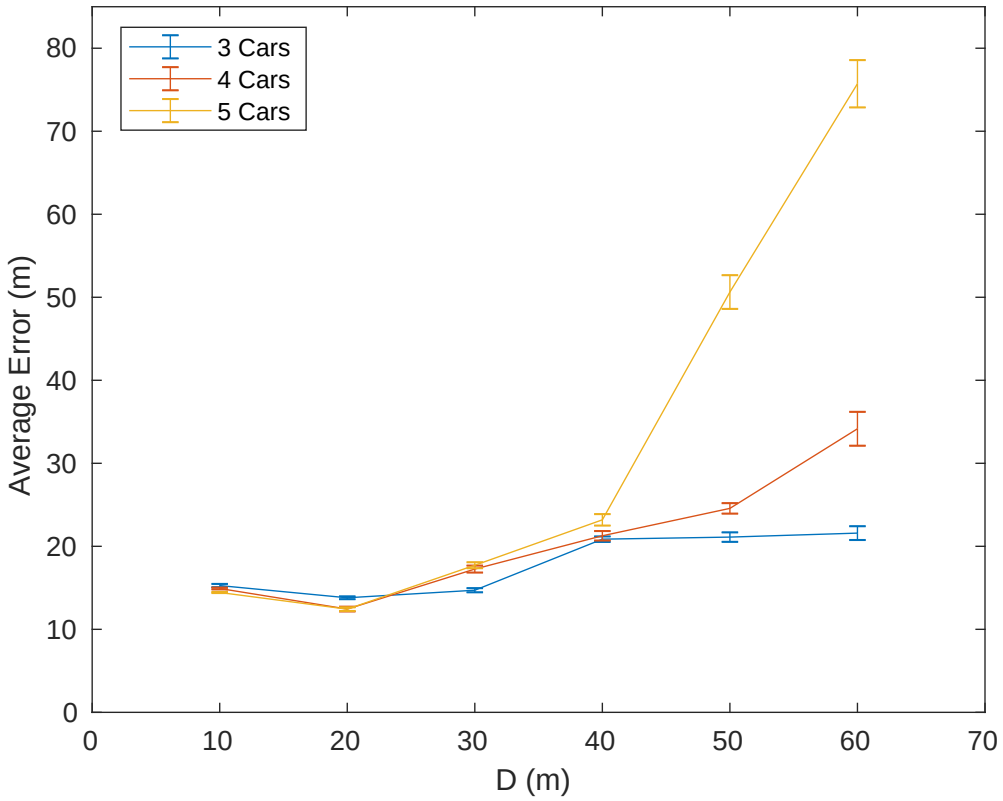

Figure 3.14: The influence of the relative receiver distance, D, on localization performance for the moving spoofer case.

Chapter 4

Evaluation Based on Experiments

4.1 Experimental Setup

In order to evaluate the effectiveness of this method in a more realistic scenario, hardware experiments were also conducted. Unfortunately, due to laws prohibiting spoofing in the open, we hard-wired the spoofer and GPS receiver and used aluminum shielding to prevent any signal leakage. To emulate the influence of Doppler shift due to the relative movement between the receiver and spoofer, we hard coded the calculated Doppler shift into the spoofer signal.

The USRP B210 from Ettus Research was used as the spoofing device which can transmit signals simultaneously over two channels. The spoofing was accomplished using the gps-sdr-sim spoofing library [6], which can be found publicly online. This library can be used to transmit a spoofing signal to any predetermined location. In this experiment it was simply transmitted with an overall frequency offset in order to represent the Doppler shift.

The receivers used in this experiment were the NEO-M8T Ublox receivers. These receivers have capabilities comparable to most standard commercial receivers. The basic experimental setup is diagrammed in figure 4.1.

After the frequencies were obtained at each measurement point they were processed using Matlab.

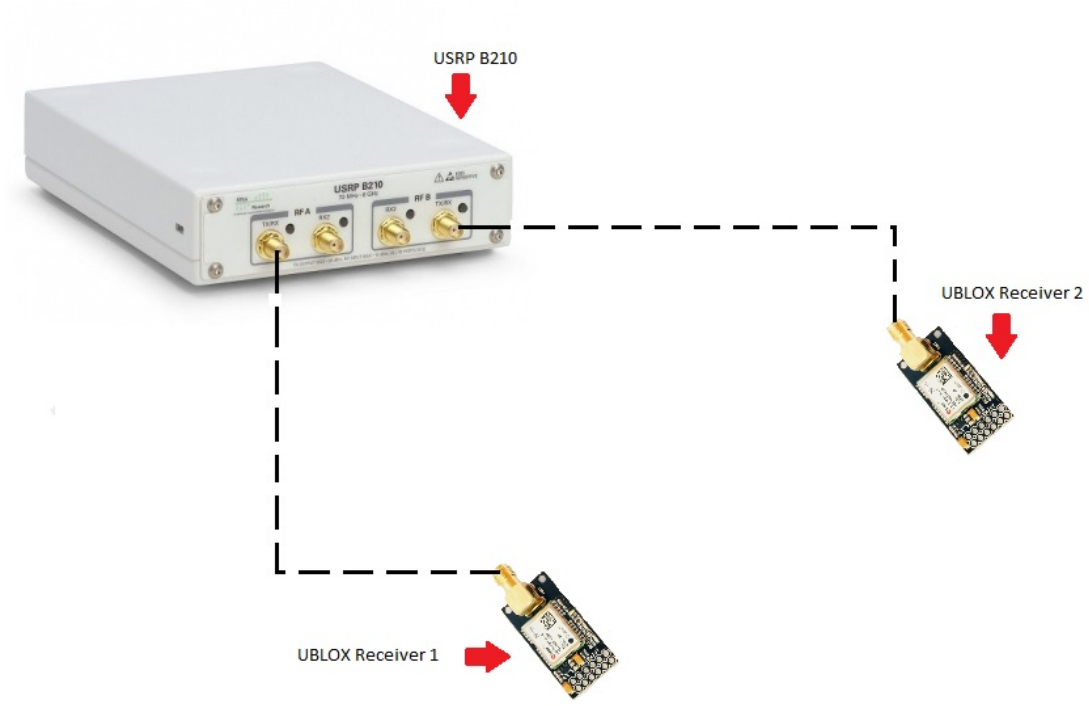

Figure 4.1: A diagram of the basic experimental setup. The USRP B210 simultaneously transmits signals over two channels to two separate GPS receivers. These would be shielded in aluminum to prevent signal leakage.

4.2 Experimental Results: Stationary Spoofer

We first evaluated the influence of perpendicular distance (A) and receiver relative distance (D) on the localization performance, with results illustrated in figure 4.2.

As can be seen in the plot, the localization error first decreases with an increase in the distance from the spoofer (A), but then increases with an increase in A. This is consistent with the numerical simulation results in figure 3.11.

Figure 4.3 displays the effect of the perpendicular distance (A) at additional distances of D that were tested. This figure once again demonstrates the trend of relatively high error with very low values of A followed by an increase in error with increasing A. Once again, this is supported by the numerical simulations.

Figure 4.4 displays the ratio of the average error to the distance from the attacker. As already discussed, there is a very large amount of error at distances very close to the attacker, such

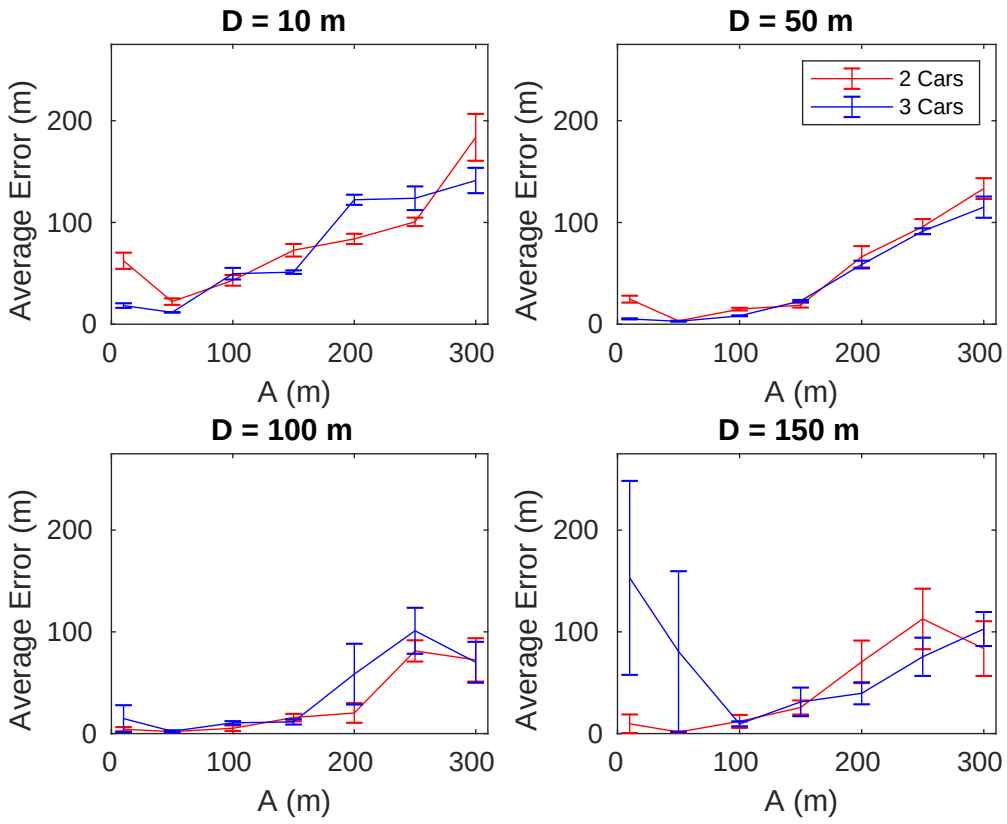

Figure 4.2: The average calculation error at different distances from the attacker and different relative vehicle distances.

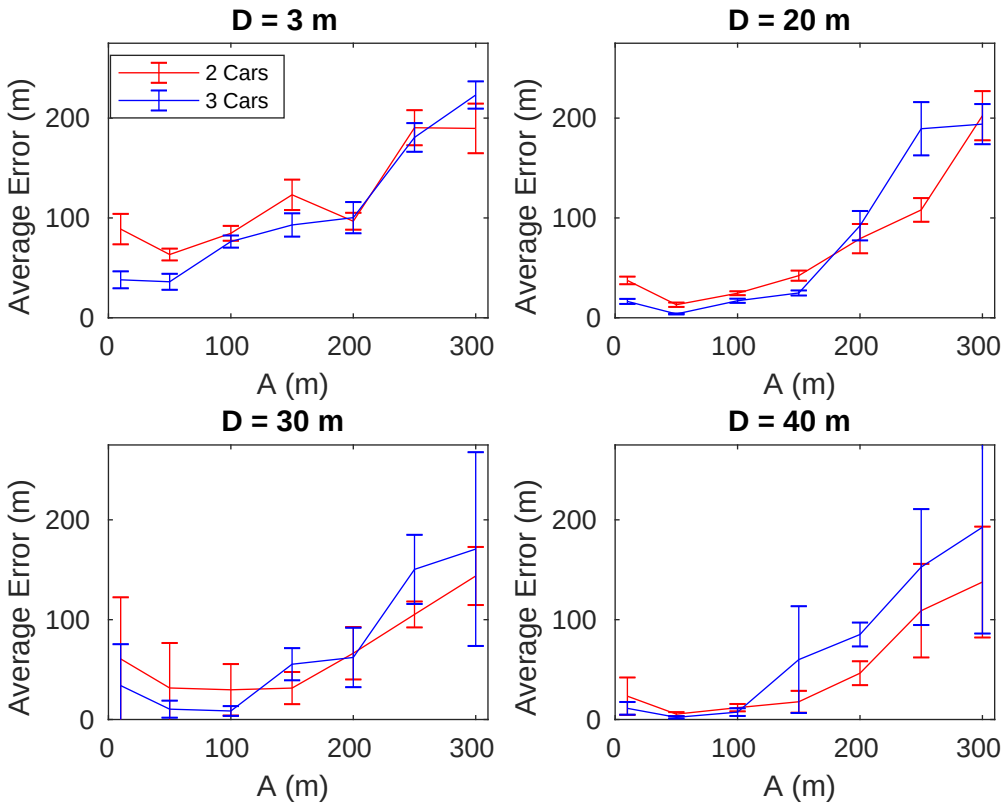

Figure 4.3: The average calculation error at additional distances from the attacker and different relative vehicle distances.

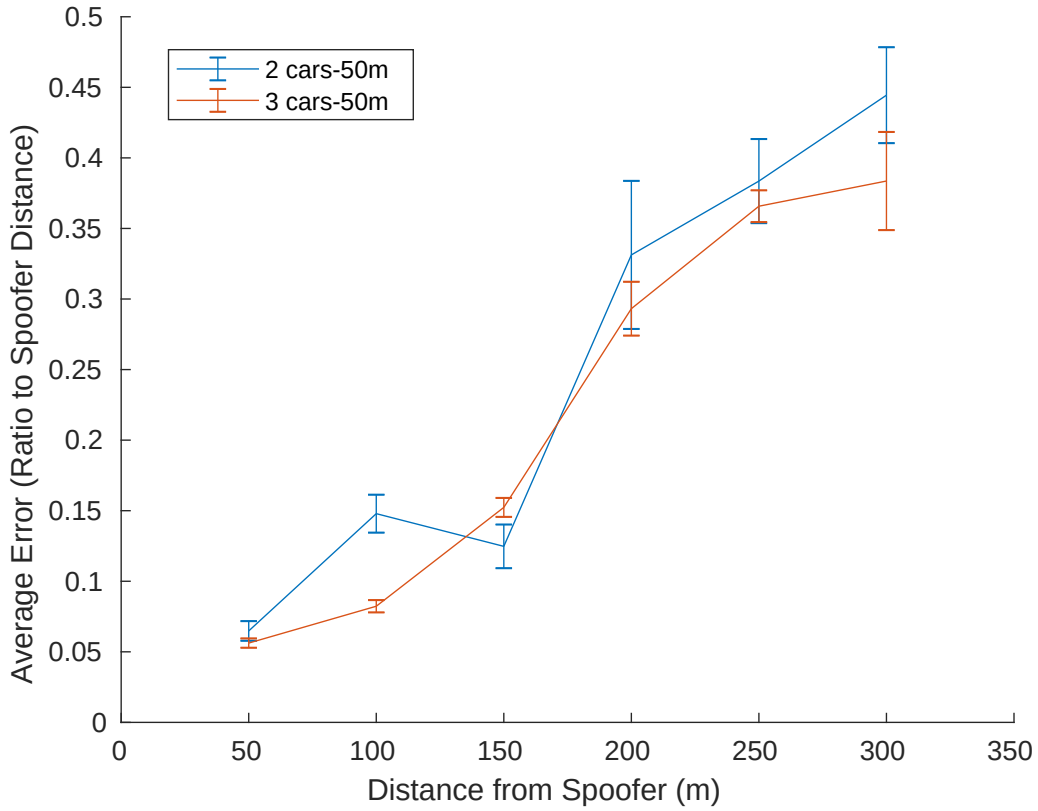

Figure 4.4: The ratio of the average calculation error to the distance from the attacker to the receivers.

as only 10 meters away. This error is not shown in figure 4.4 as it is large enough to obscure the rest of the trends. After the large error however, there is a dramatic decrease in error leading to the least relative error at a distance of 50 meters away from the attacker. Then, there is a gradual increase in relative error as the distance from the attacker increases. This means that the algorithm is actually becoming less accurate as the attacker distance increases, and is especially inaccurate at very low values of A. Therefore, depending on the required precision, this method seems best suited for an attacker distance between about 50 and 200 meters. Figure 4.4 only displays the data for a relative vehicle distance of 50 meters, but the trends remains similar for all relative vehicle distances.

The influence of relative distance between vehicles, D, on the localization performance was also evaluated. The results are given in figures 4.5 and 4.6. This demonstrates the patterns found in changing distances in between receivers. As can be seen, the general trend is fairly consistent

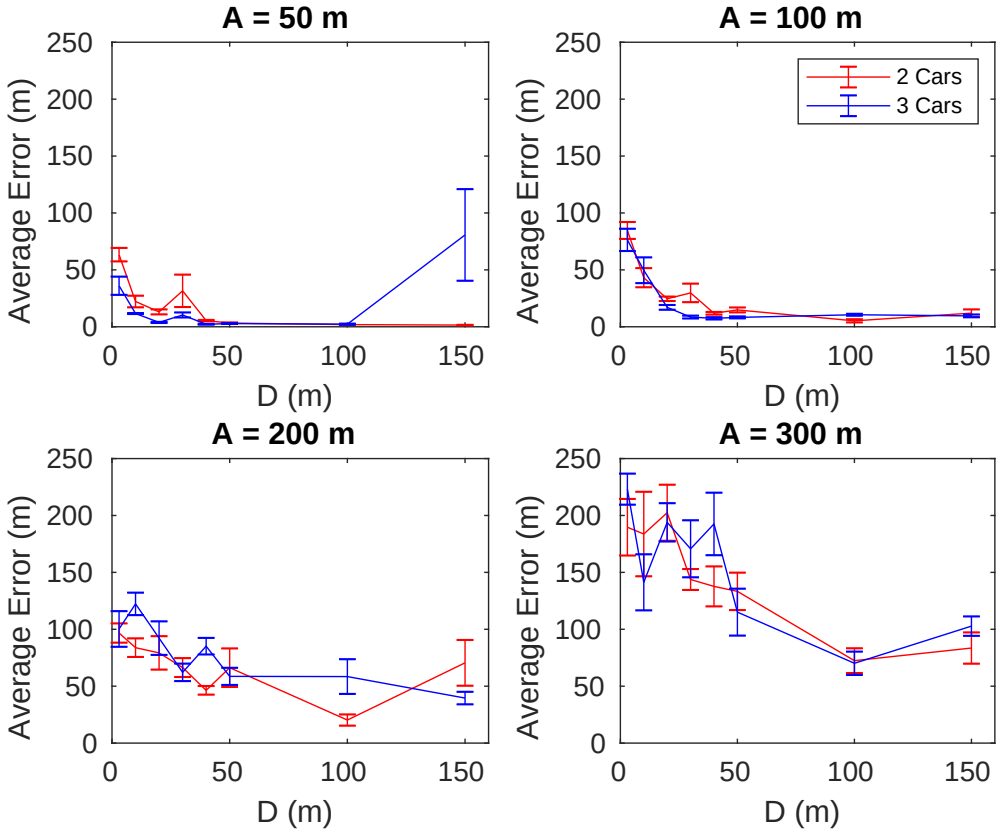

Figure 4.5: The average calculation error at different perpendicular distances from the attacker and different relative vehicle distances.

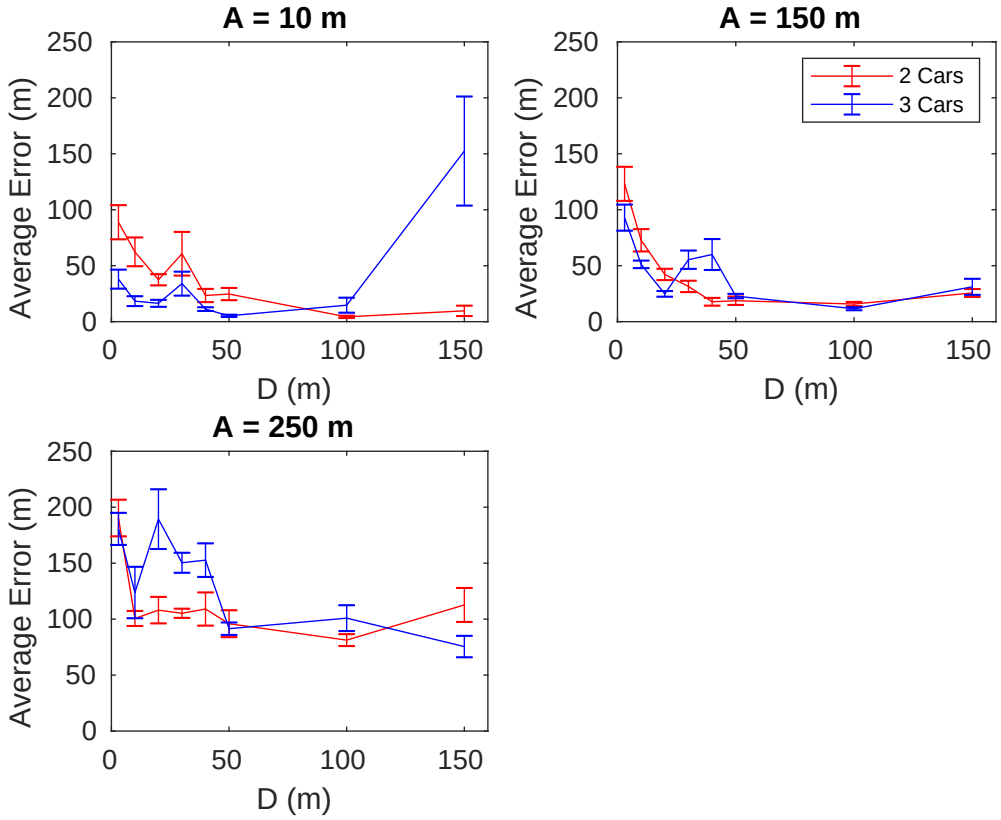

Figure 4.6: The average calculation error at additional perpendicular distances from the attacker and different relative vehicle distances.

regardless of distance from the attacker. More specifically, the localization error first decreases and then increases with an increase in the relative distance, which is consistent with the numerical simulation results in figure 3.13.

Once again, it was desired to see the trend as a ratio of the error to the distance to the attacker. Therefore, figure 4.7 displays this ratio at different values of D, the relative receiver distance. Figure 4.7 specifically shows the error ratio at an Attacker distance of 50 meters.

As can be seen, figure 4.7 confirms the trend that average error tends to decrease as D increases. However, after a certain point the process begins to break down and error increases dramatically. Furthermore, the three car case breaks down before the two car case, which was an effect observed in the numerical simulations seen in 3.13 as well.

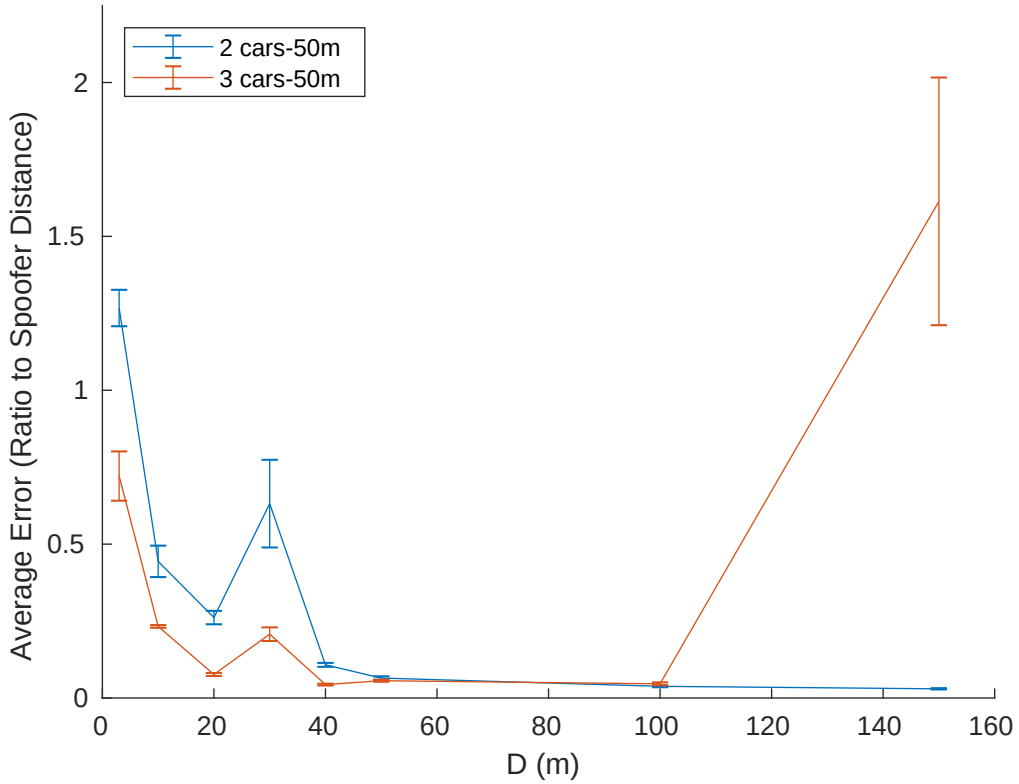

Figure 4.7: The ratio of the average calculation error to the distance from the attacker to the receivers at different relative receiver distances.

4.3 Experimental Results : Mobile Spoofer

Due to time constraints, more limited experiments were conducted for the moving spoofer scenario. Instead of examining multiple variables across a set range of values, the moving spoofer case was only evaluated experimentally in two main cases. These two cases were based on the formations displayed in figures 3.5 and 3.6, with each victim being 50 meters apart. Once again, the experiments were conducted by using the USRP B210 to transmit signals to the receivers with the calculated Doppler shift hard coded in.

Figure 4.8 displays the error calculated at each time instance for the moving spoofer in the opposite direction of the victims. As can be seen, the error starts at five meters, but then steadily increases with each successive position. This is because there is some error when calculating the magnitude and direction of the spoofer's motion, which propagates throughout the calculated posi-

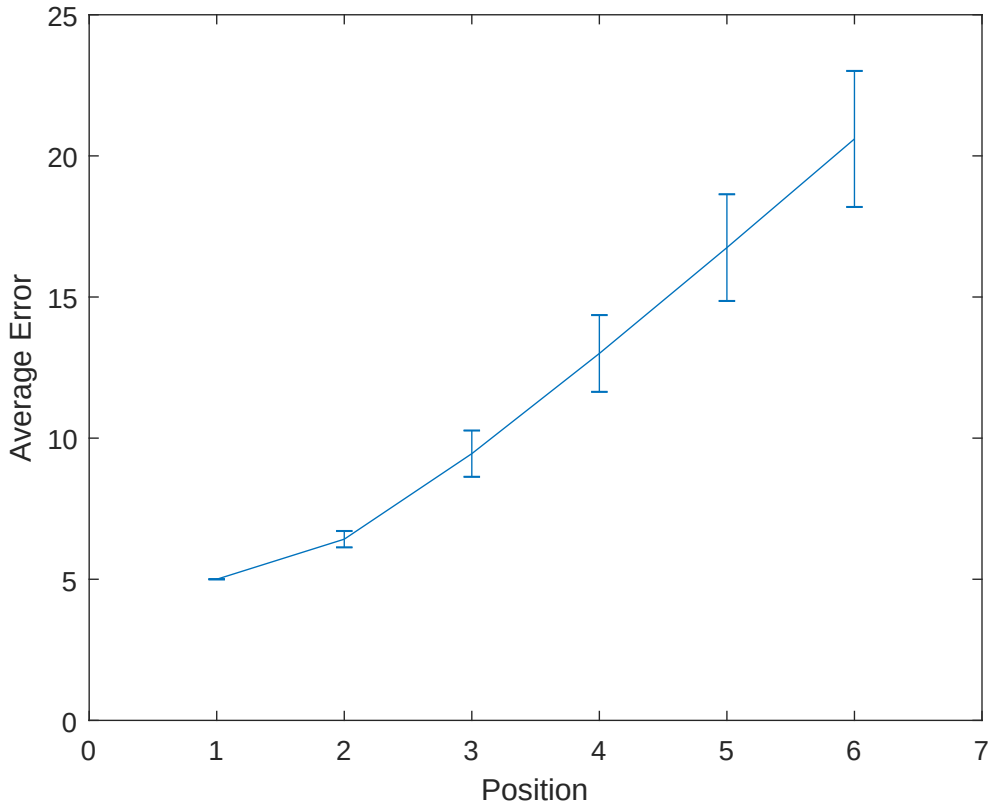

Figure 4.8: The average error calculated for each position based on experiments for the moving spoofer on the same road in the opposite direction of the victims.

tions. The first position always has an error of exactly five meters because while the vertical starting point is calculated correctly, the algorithm consistently determines that the spoofer is directly inline with the victims, while it really has an attacker distance of five meters. This could possibly be improved by using finer steps when iterating initial values, as in this experiment the steps were all the size of ten meters. However, this would lead to longer processing times.

Overall, the calculation error at any position for this formation is always less than 25 meters for any position. This is definitely sufficient for helping the authorities locate the spoofer. However, it should be noted that this only works if the attacker passes the victims. Otherwise the same problem exists as in the case where the spoofer is moving in the same direction as the victims: the Doppler shift is never changing so it is impossible to come to a solution.

Figure 4.9 displays the calculation error from the case where the spoofer moves at a 45 degree

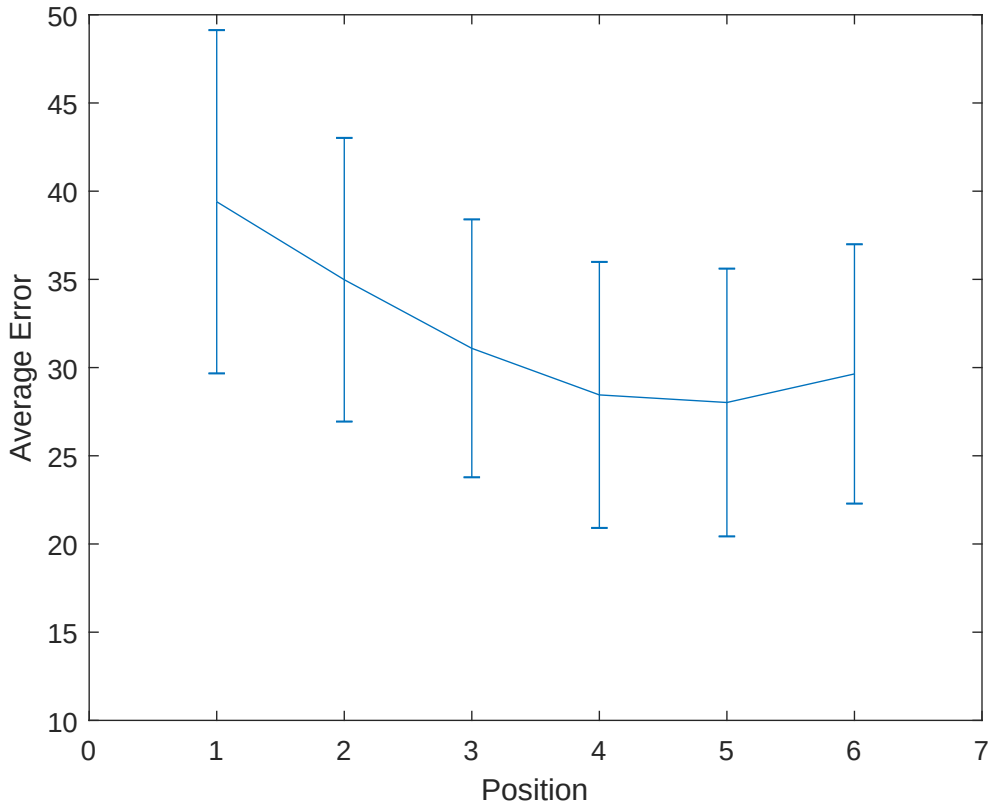

Figure 4.9: The average error calculated for each position based on experiments for the moving spoofer moving at a 45 degree angle relative to the victims.

angle relative to the victims. The error in this formation is consistently higher than that encountered in the previous formation. Furthermore, in this case the error decreases the first few positions before once again increasing. The decrease in error is due to the fact that the error calculated for the first position is in the opposite direction of the error calculated in the motion of the spoofer. This is not guaranteed to happen, but in the five trials run did lead to a decrease in calculated error through the first few positions.

All positions in figure 4.9 have calculated errors between 20 and 50 meters, and must calculated errors are between 30 and 40 meters. Once again, this should be a reasonable enough range to greatly narrow down the possible locations of the spoofer. This is especially true when it is considered that the spoofer is traveling along a road, which helps further narrow down its possible locations. Therefore, in both cases it is possible to calculate the position of the spoofer to a

reasonable degree of accuracy.

Chapter 5

Conclusions

5.1 Evaluation of Results

In this paper we propose using a network of cooperative vehicles to localize a spoofing attacker through use of their respective Doppler shifts. Each vehicle takes Doppler measurements over a short period of time, and then based on the changes in each Doppler shift a system of equations can be generated. Minimizing the error in this system of equations reveals an estimate of the location of the attacker.

The methods proposed in this paper have been demonstrated to be effective under certain circumstances. For the stationary attacker, when the distance from the attacker is between about 50 and 200 meters and the relative distance between vehicles is between about 50 and 100 meters, the ratio of the calculation error to the attacker distance is typically less than 0.2. This does not precisely localize the attacker, but it does greatly narrow down the possible locations. This would permit authorities to have a much smaller search radius, and thus a much easier time finding an attacker.

For the moving spoofer, the algorithm was able to calculate the position of the spoofer to within 50 meters of error regardless of whether the attacker was moving the other direction of the victims or on a different road that crosses with the victims. However, this does require making a number of assumptions, such as the fact that the spoofer is moving at a relatively constant velocity in a constant direction. Furthermore, this method is limited in that it will not work if the attacker is moving in the same direction at the same speed as the victims, which is unfortunately quite likely

if the spoofer is on the same road as the victims. Therefore, the algorithm proposed in this paper is capable of localizing moving attackers, although it does have some significant limitations.

5.2 Future Work

As mentioned previously, all the data in this paper was gathered in laboratory simulations. Thus, moving forward this method would have to be tested under more realistic conditions, which would require permission to spoof GPS signals in an open environment. Under such conditions the noise from the spoofer will no longer be an issue (the transmitted signal will definitely be the same for every receiver at a given point in time), although there will be some additional noise in the position and velocity of each vehicle. The amount of noise in those areas would depend on the accuracy of the odometer readings. Therefore, it is expected that the results would be similar to those encountered in this paper, but further testing would be required to ensure this. Furthermore, in a real world scenario the receivers should be able to record more than the minimum number of required data points. As demonstrated by the numerical simulations for both the stationary and moving spoofer cases, with more samples the accuracy of the process can be improved at least slightly.

This method can also be generalized in a few ways. First, in this paper it is assumed that all vehicles are moving in a perfectly straight line. At times this would be a reasonable approximation, as cars should be following roads, which are generally fairly straight. However, some roads curve or turn and this method does not currently account for that. It would be possible for the mathematics to be generalized to allow cars to turn, although this would require each car to be able to determine its turning angle. This information is not readily available through the odometer for most vehicles, so this generalization would be significantly more difficult to implement.

This method also makes numerous assumptions about the moving spoofer, as previously mentioned. Without these assumptions the number of variables required increases greatly, which requires the use of more vehicles and measurements. Furthermore, as the complexity of the system of equations increases so too does the processing time required to solve it. As such, it is currently not practical to solve for a spoofer moving without restrictions. Unfortunately, in order to be actually implemented this is a problem that would need to be solved.

5.3 Conclusions

In conclusion, the algorithm proposed in this paper works effectively for localization of stationary attackers within certain distance ranges. It also shows promise for localization of moving spoofers, although more work would be required to get around the necessary restrictive assumptions. This method also still needs to be tested in real world environments and would require a network of vehicles, but could prove to be an affordable means of detection and localization of GPS spoofing attacks.

Bibliography

[1] Authenticating gnss: Proofs against spoofs, part 2. In *Inside GNSS*, pages 71–78, September/October 2007.

[2] Massive gps jamming attack by north korea. https://www.gpsworld.com/massive-gps-jamming-attack-by-north-korea/, 2012.

[3] Ut austin researchers successfully spoof an 80 million dollar yacht at sea. https://news.utexas.edu/2013/07/29/ut-austin-researchers-successfully-spoof-an-80-million-yacht-at-sea/, 2013.

[4] u-blox m8 concurrent gnss timing modules. https://www.u-blox.com/sites/default/files/NEO-LEA-M8T-FW3_DataSheet_%28UBX-15025193%29.pdf, 2016.

[5] Opensky network. https://opensky-network.org, 2017.

[6] Software-defined gps signal simulator. https://github.com/osqzss/gps-sdr-sim, 2017.

[7] Ns-raw : Carrier phase raw measurement output gps receiver. http://navspark.mybigcommerce.com/ns-raw-carrier-phase-raw-measurement-output-gps-receiver/, 2018.

[8] Piksi multi gnss module. https://www.swiftnav.com/store/gnss-sensor-volume-orders/piksi-multi-gnss-module?, 2018.

[9] J. Bhatti and T. Humphreys. Hostile control of ships via false gps signals: Demonstration and detection. In *The University of Texas at Austin, Tech. Rep.*, 2014.

[10] John A. Volpe National Transportation Systems Center. Vulnerability assessment of the transportation infrastructure relying on the global positioning system. In *Tech. Rep. Final Report*, August 2001.

[11] B. O'Hanlon et al. Real-time spoofing detection in a narrow-band civil gps receiver. In *Proceedings of the 23rd International Technical Meeting of the Satellite Division of The Institute of Navigation (ION GNSS 2010)*, pages 2211–2220, September 2010.

[12] F. Fasching. Raspignss aldebaran. https://drfasching.com/products/gnss/raspignss.html, 2018.

[13] W. Franz and H. Hartenstein. Inter-vehicle communications, fleetnet project. In *University Karlruhe*, 2005.

[14] L. Heng, D. Work, and G. Gao. Gps signal authentication from cooperative peers. In *IEEE Transactions on Aerospace and Electronic Systems Vol. 49, No. 4*, October 2013.

[15] T. Humphreys. Statement on the vulnerability of civil unmanned aerial vehicles and other systems to civil gps spoofing. In *The University of Texas at Austin, Tech. Rep.* Submitted to the House Committee on Homeland Security, July 2012.

[16] T. Humphreys, B. Ledvina, M. Psiaki, B. O'Hanlon, and P. Kinter Jr. Assessing the spoofing threat: Development of a portable gps civilian spoofer. In *International Technical Meeting of the Satellite Division of the Institute of Navigation, ser. ION GNSS '08*, pages 2314–2325, September 2008.

[17] U. Hunkeler, J. Colli-Vignarelli, and C. Dehollain. Effectiveness of gps-jamming and countermeasures. pages 1–4. Proc. Int. Conf. Localization GNSS, 2012.

[18] K. Jansen, M. Schafer, D. Moser, V. Lenders, C. Popper, and J. Schmitt. Crowd-gps-sec: Leveraging crowdsourcing to detect and localize gps spoofing attacks. In *IEEE Symposium on Security and Privacy (SP)*, 2018.

[19] K. Jansen, N. Tippenhauer, and C. Popper. Multi-receiver gps spoofing detection: Error models and realiztion. In *Annual Computer Security Applications Conference, ser. ACSAC '16*, pages 237–250. ACM, December 2016.

[20] A. Kerns, D. Shepard, J. Bhatti, and T. Humphreys. Unmanned aircraft capture and control via gps spoofing. In *Journal of Field Robotics, vol. 31, no. 4*, pages 617–636, July 2014.

[21] M. Kuhn. An assymetric security mechanism for navigation signals. In *Proc. 6th Int. Conf. IH*, pages 239–252, 2004.

[22] G. Liu, R. Zhang, C. Wang, and L. Liu. Synchronization-free gps spoofing detection with crowdsourced air traffic control data. In *20th IEEE International Conference on Mobile Data Management (MDM)*, 2019.

[23] S. Lo, D. De Lorenzo, P. Enge, D. Akos, and P. Bradley. Signal authentication, a secure civil gnss for today. In *Inside GNSS, Vol. 4, No. 5*, pages 30–39, September/October 2009.

[24] P. Misra and P. Enge. Global positioning system: Signals measurements and performance. USA:Ganga-Jamuna Press, 2006.

[25] P. Montgomery, T. Humphreys, and B. Ledvina. Receiver autonomous spoofing detection: Experimental results of a multiantenna receiver defense against a portable civil gps spoofer. In *International Technical Meeting of the Institute of Navigation, ser. ION '09*, pages 124–130, January 2009.

[26] D. Namowitz. Gps jamming expected in southeast during military exercise. https://www.aopa.org/news-and-media/all-news/2020/january/14/gps-jamming-expected-in-southeast-during-military-exercise, 2020.

[27] T. Nightswander, B. Ledvina, J. Diamond, and R. Brumley. Gps software attacks. In *ACM Conference on Computer and Communications Security, ser. CCS '12*, pages 450–461. ACM, October 2012.

[28] P. Papadimitratos and A. Jovanovic. Gnss-based positioning: Attacks and countermeasures. In *IEEE Military Communications Conference, ser. MILCOM '08*, pages 1–7. IEEE, November 2008.

[29] O. Pozzobon. Keeping the spoofs out, signal authentication services for future gnss. In *Inside GNSS, vol. 6, no. 3*, pages 48–55, May/June 2011.

[30] M. Psiaki and T. Humphreys. Gnss spoofing and detection. In *Proceedings of the IEEE, vol. 104, no. 6*, pages 1258–1270, April 2016.

[31] M. Psiaki, B. O'Hanlon, J. Bhatti, D. Shepard, and T. Humphreys. Gps spoofing detection via dual-receiver correlation of military signals. In *IEEE Transactions on Aerospace and Electronic Systems Vol. 49, No. 4*, October 2013.

[32] M. Psiaki, B. O'Hanlon, S. Powell, J. Bhatti, K. Wesson, T. Humphreys, and A. Schofield. Gnss spoofing detection using two-antenna differential carrier phase. In *International Technical Meeting of The Satellite Division of the Institute of Navigation, ser. ION GNSS+ '14*, pages 2776–2800, September 2014.

[33] A. Ranganathan, H. Olafsdottir, and S. Capkun. Spree: A spoofing resistant gps receiver. In *ACM Conference ib Mobile Computing and Networking, ser. MobiCom '16*, pages 348–360. ACM, October 2016.

[34] M. Russon. Wondering how to hack a military drone? it's all on google. http://www.ibtimes.co.uk/wondering-how-hackmilitary-drone-its-all-google-1500326, 2015.

[35] L. Scott. Anti-spoofing and authenticated signal architectures for civil navigation systems. In *Proc. 16th Int. Tech. Meet. Satell. Div. ION GPS/GNSS*, pages 1543–1552, September 2003.

[36] C. Sebastian. Getting lost near the kremlin? russia could be 'gps spoofing'. https://money.cnn.com/2016/12/02/technology/kremlin-gps-signals/, 2016.

[37] P. Swaszek and R. Hartnett. Spoof detection using multiple cots receivers in safety critical applications. In *International Technical Meeting of The Satellite Division of the Institute of Navigation, ser. ION GNSS+ '13*, pages 2921–2930, September 2013.

[38] P. Swaszek, R. Hartnett, M. Kempe, and G. Johnson. Analysis of a simple, multi-receiver gps spoof detector. In *International Technical Meeting of The Institute of Navigation, ser. ION '13*, pages 884–892, January 2013.

[39] N. Tippenhauer, C. Popper, K. Rasmussen, and S. Capkun. On the requirements for successful gps spoofing attacks. In *ACM Conference on Computer and Communications Security, ser. CCS '11*, pages 75–86. ACM, October 2011.

[40] J. Tsui. Fundamentals of global positioning system receivers: A software approach. 2000.

[41] D. Yu, A. Ranganathan, T. Locher, S. Capkun, and D. Basin. Short paper: Detection of gps spoofing attacks in power grids. In *ACM Conference on Security and Privacy in Wireless and Mobile Networks, ser. WiSec '14*, pages 99–104. ACM, July 2014.